
**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

DEPARTAMENTO DE TELECOMUNICACIONES


# DISEÑO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA (WLAN) PARA LA FACULTAD DE INGENIERÍA BAJO EL ESTÁNDAR IEEE 802.11

**TESIS**

QUE PARA OBTENER EL TÍTULO DE

**INGENIERO EN TELECOMUNICACIONES**

PRESENTA


**EMMANUEL ADÁN DÍAZ PÉREZ**



Asesor: Ing. Jesús Reyes García

Ciudad Universitaria, 2005

# Agradecimientos

*Agradecer significa para mí, otorgar el reconocimiento que se merecen todas aquellas personas que me han apoyado para conseguir esta meta. También es un sentimiento, y esto hace que sea difícil expresarlo en palabras, porque a pesar de la sinceridad y del valor que quisiera plasmarles, nunca serán suficientes para describir todos aquellos pensamientos que llegan a mi mente y que evocan esos gratos recuerdos de su presencia.*

*Aún así, quisiera dejar escrito los siguientes agradecimientos y dedicatorias. A mi abuela Juana, que me brindó todo su amor, cariño y cuidado desde que era pequeño. A Miguel, que nunca dejó de apoyarme y que siempre me brindó toda su confianza para lograr esta meta tan anhelada. A mis padres y a mi mejor amigo: mi hermano Julio, compañero inseparable en todos estos años. A mi abuelo Roberto, Carmen, Beto, Tere, Luz, Ángeles y Luis, que me trataron siempre como a un hermano y que estuvieron a mi lado en todo momento. A Fernando, Jacinto y a mi cuñada Lulú que también ya son parte de la familia. A mi sobrina Naela, que recién comienza su hermosa vida. A mis primos Memo, Adrián, Luis, Juan José, Mauricio, Sergio y Marcos, porque a su lado he vivido gratos momentos.*

*También mis amigos merecen agradecimiento. A Myrna, que es mi más antigua confidente. A Víctor, Memo, Alonso, Leo, Rafael, Jorge, Narciso, Ernesto, Alberto y Alfonso, cuya amistad atesoro desde mi paso por la preparatoria y que hasta el día de hoy sigo conservando. Agradezco también a mi querida Ana María, porque sus palabras de aliento siempre me ayudaron a salir a flote en las situaciones más difíciles. A Melina, Liliana y Thalía, que siempre tuvieron el tiempo para escucharme y brindarme su más sincera amistad. Más recientemente, les agradezco su amistad a mis compañeros de oficina: A Bety, por darme ánimos para terminar este trabajo a pesar de mi fatiga. A Sergio, a Saúl y a Nazia, que me han dado su amistad de manera incondicional. A mi jefe Guillermo, por otorgarme los permisos necesarios para concluir este proyecto.*

*En lo académico, quisiera agradecer a mi alma mater, la Universidad Nacional Autónoma de México, que me dio la oportunidad de estudiar en sus aulas. A mi asesor de tesis Jesús Reyes, cuyo consejo siempre se tradujo en mejora para esta tesis. A mis maestros, que me hicieron sentir orgulloso de ser universitario. A Noé Cruz Marín, Alejandro Velázquez Mena y a Eduardo Díaz, que me brindaron información muy valiosa para que este proyecto tuviera sentido.*

*Existen muchas más personas que por falta de espacio no están aquí, pero que sin duda, están en mi mente.*

*Por eso y mucho más, gracias por su amor, por su amistad, por su sinceridad, por su comprensión, y sobre todo, por formar parte de mi vida.*

*En nosotros reside el anhelo*
*De alcanzar la verdad y el saber*
*Nuestras alas presienten el vuelo*
*De la ciencia, el amor y el deber*
*Que nos guíe la voz del maestro*
*A alcanzar el sublime ideal*
*Y un mañana de luz será nuestro*
*De la patria diadema triunfal*
*Universidad, Universidad*
*Por mi raza el espíritu hablará.*

Fragmento del Himno de la
Universidad Nacional Autónoma de México

# Índice

**Capítulo Tres. El Estándar IEEE 802.11**



**Capítulo Cuatro. Subcapa de Control de Acceso al Medio (MAC)**

**Capítulo Cinco. Seguridad en las WLAN's**



**Capítulo Seis. Diseño y Propuesta de Implementación de la WLAN**

# Introducción

Actualmente las Redes de Área Local (LAN) han permitido el intercambio eficiente de información electrónica entre usuarios que se encuentran dentro de un mismo entorno, cuando los dispositivos involucrados se ubican dentro de una distancia relativamente pequeña. Una prueba de ello es que gran parte de las empresas privadas, instituciones educativas y gubernamentales, entre otras, cuentan con una infraestructura LAN, gozando ampliamente de sus beneficios.

La aceptación de ésta tecnología se debe en gran parte a su facilidad de implementación y al desarrollo continuo de nuevos productos, dando como resultado que las soluciones sean de bajo costo.

Dentro de las tecnologías mas utilizadas para la implementación de una Red LAN se encuentra Ethernet, la cual ha tenido gran éxito debido a su simplicidad de operación y alta velocidad de transmisión de datos comúnmente a 10 Mbps y 100 Mbps, empleando con mayor frecuencia el cable de par trenzado para la implementación física.

Existen más formas de implementar una Red LAN, pero todas ellas tienen en común el uso de cable de cobre o fibra óptica. Una de las ventajas del cableado radica en que es poco vulnerable al ruido, y generalmente se opta por emplear cable que cuente con blindaje electromagnético (en el caso del par trenzado), y en el caso de cable coaxial o fibra óptica ésta característica es inherente.

Sin dejar a un lado todos los beneficios de las Redes LAN, resultan evidentes ciertas limitaciones en una implementación con cableado estructurado. Entre ellas podemos mencionar:

- Se necesita diseñar minuciosamente la estructura del cableado. Esto representa dificultades para aquellos edificios en donde no sea sencillo modificar su configuración original debido a su antigüedad, por citar un ejemplo. En algunas ocasiones también resulta complicado diseñar una red donde los equipos que se contemplan, estarán situados a grandes distancias.

- Una vez que se ha hecho el cableado, los usuarios tienen que estar en un punto fijo para poder hacer uso de los servicios que presta la red.

- Se requiere de personal altamente capacitado par llevar a cabo la configuración y mantenimiento del equipo.

- Si se requiere reubicar a los usuarios de la red o a toda ella, es necesario rediseñar la red, que en algunos casos implica la pérdida del cable utilizado con anterioridad, ya que puede quedar inoperante.

Éstas limitantes se han convertido en nuevas necesidades de los usuarios. Ahora ya no es suficiente con poder acceder a la información, sino que se requiere que sea en cualquier lugar disponible.

Para hacer esto posible, se ha comprobado la utilidad de las tecnologías inalámbricas. Las comunicaciones inalámbricas surgieron con el lanzamiento de la radio y la televisión. En ese entonces, no existía intercambio de información pues el sistema comprendía únicamente de un transmisor y un receptor. En otras palabras, la comunicación se efectuaba en un solo sentido.

Actualmente se tiene en el mercado una infinidad de productos que emplean las comunicaciones inalámbricas de una o dos vías, cuestión que ha impulsado el desarrollo de nuevas tecnologías de información enfocadas a resolver las necesidades de los usuarios en este sentido. Es así como nacen las Redes de Área Local Inalámbricas, que resuelven en gran parte los inconvenientes de las implementaciones LAN.

Las Redes Inalámbricas tienen la principal característica de ofrecer la movilidad de los usuarios, es decir, que la conexión de los dispositivos dentro del entorno inalámbrico se mantendrán "conectados" aunque el usuario cambie su posición constantemente.

Cuando se aprueba el primer Estándar para marcar los lineamientos mínimos necesarios de interoperabilidad entre dispositivos, se vislumbraba lejano el tiempo en que se pudiera comparar el desempeño de las redes inalámbricas con las LAN tradicionales, pues las tasas de transmisión eran alrededor de 1 y 2 Mbps.

A seis años de este acontecimiento, se puede asegurar que se pueden emplear las mismas aplicaciones de las redes LAN en la nueva tecnología inalámbrica, y que sin duda, llegará el momento en que no existirán diferencias significativas entre ambos tipos de Red.

Es por ello que en la presente tesis se tiene como objetivo diseñar una Red inalámbrica que proporcione el acceso a los servicios de red que actualmente brindan los laboratorios de cómputo a los estudiantes de la Facultad de Ingeniería, tomando como base los principios que maneja el Estándar IEEE 802.11, y cuya estructura sea compatible con la Red LAN que actualmente opera en dichos laboratorios.

A través del siguiente texto se estudiarán los diversos elementos que constituyen a las Redes Inalámbricas, con la intención de abordar los temas competen a su funcionamiento y analizando las principales premisas de diseño.

En el Capítulo 1 se hace mención del origen de las Redes Inalámbricas, sus formas de implementación de manera general y la justificación a la elección de esta tecnología para la Red propuesta.

En el Capítulo 2 se estudian las técnicas de Espectro Disperso así como las técnicas de modulación y codificación que toman lugar en la operación de las Redes Inalámbricas.

En el Capítulo 3 se hace un breve análisis del Estándar 802.11 y sus respectivos grupos de trabajo: 802.11a, 802.11b y 802.11g. Dicho análisis se enfoca a la Capa 1 (Capa Física) del modelo de Referencia OSI, ya que la capa 2 (Capa de Enlace, subcapa MAC) es analizada en el Capítulo 4 tomando como base los mismos Estándares.

En el Capítulo 5 se aborda el tema de la seguridad en las Redes Inalámbricas, el cual contiene diferencias significativas respecto a la seguridad en las redes LAN tradicionales.

Por último, en el Capítulo 6 se realiza la propuesta de implementación de la Red, tomando en consideración la teoría previamente analizada, además de las principales premisas de diseño.

CAPÍTULO UNO

# Redes de Área Local Inalámbricas: WLAN's

## 1.1 Definición

Una Red Inalámbrica de Área Local se puede definir como un conjunto de dispositivos electrónicos situados en un entorno geográfico limitado, capaces de intercambiar información digital entre sí, utilizando el aire como canal de comunicación.

En las redes de datos tradicionales (sistemas alámbricos) ésta información viaja a través de cables. Una Red de Área Local Inalámbrica, también llamada WLAN (Wireless Local Area Network), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red alámbrica. Las WLAN emplean ondas electromagnéticas (radiofrecuencias e infrarrojos) como instrumento para la transmisión de datos, minimizando así la necesidad de conexiones con cable y permitiendo de esta manera al usuario la posibilidad de cambiar su ubicación arbitrariamente y sin perder la conectividad con la Red.

## 1.2 Antecedentes

Como resultado de diversas investigaciones que tenían por objeto la transmisión de datos utilizando medios inalámbricos, surgen las Redes Inalámbricas de Área Local. El origen de las WLAN's se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, que consistió en utilizar enlaces por medio de infrarrojos para crear una red local dentro de una fábrica. Estos resultados, publicados por el IEEE[1], pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante utilizando infrarrojos y microondas, bajo el esquema de Espectro Disperso (SS)[2]. La técnica de espectro disperso es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es poco susceptible al ruido y produce pocas interferencias. En mayo de 1985 y

[1] Institute of Electrical and Electronics Engineers
[2] Spread Spectrum

tras cuatro años de estudios, la FCC[3], agencia federal del Gobierno de Estados Unidos encargada de la regulación y administración en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical)[4] 902 – 928 MHz, 2.400 – 2.4835 GHz y 5.725 – 5.850 GHz, las cuales permiten la operación de las redes inalámbricas con una potencia menor a 1 W y son consideradas como libres de licencia. A pesar de la conveniencia del uso de estas bandas sin necesidad de licitarlas y de la facilidad de proveer servicios de acceso multiusuario, una de las principales desventajas se ve reflejado en el desempeño de la red, que puede verse afectado si no se tiene cuidado de evitar las interferencias con otros usuarios u equipos que emplean la misma banda.

La actividad para lograr un estándar marchó a un ritmo muy lento y no fue sino hasta Octubre de 1997 cuando finalmente se completó el estándar para Redes de Área Local Inalámbricas, concretándose así el Estándar IEEE 802.11. En el presente texto, nos referiremos al mismo únicamente como *Estándar 802.11* por razones de simplicidad.

Organizaciones como el Comité 802 del IEEE continúan en el desarrollo de nuevas regulaciones en materia de Redes de Información. En fechas recientes se han creado nuevos estándares por parte de este comité, con el fin de proponer nuevas alternativas y mejorar las existentes en materia de velocidades de transmisión y en el uso de diferentes bandas de frecuencia, así como mecanismos de seguridad. Otras organizaciones juegan un papel importante en la adopción de las redes inalámbricas. La Alianza para la Compatibilidad de Ethernet Inalámbrico (WECA)[5] es la más notable de dichas organizaciones. El IEEE y la WECA han impulsado la innovación y migración hacia los estándares que se hacen referencia, con el objeto de que la industria acepte de manera exitosa dichas recomendaciones.

## 1.3 Principios del Funcionamiento de las WLAN's

Es relativamente sencillo utilizar redes inalámbricas bajo el Estándar 802.11 e integrarlas a las redes alámbricas que se encuentren operando con el Estándar 802 para lograr extender la interconectividad de los usuarios. Esto significa que la gran mayoría de los servicios ofrecidos por las redes alámbricas tales como compartir archivos, envío de correos electrónicos y la navegación por Internet, se encuentran disponibles en las redes WLAN.

[3] Federal Communications Comission
[4] En México se definen como bandas ICM refiriéndose a las bandas de frecuencias para uso Industrial, Científico y Médico
[5] Wireless Ethernet Compatibility Alliance

La clave del funcionamiento de una WLAN son las células. La célula es el área donde todas las comunicaciones inalámbricas toman lugar. El Estándar 802.11 denomina a éstas células como Conjunto de Servicios Básicos (BSS)[6]. En general una célula cubre un área más o menos circular. Dentro de cada célula existe un administrador de tráfico de información llamado Punto de Acceso (AP)[7]. El número de equipos inalámbricos por célula es dependiente de la cantidad del tráfico y/o del tipo de datos.

Para redes de mayor extensión (en cuanto a número de usuarios y/o área de cobertura) se pueden formar multicélulas conectando muchos AP's con antenas direccionales externas en lugar de usar las antenas omnidireccionales incluidas en los AP's. Esta opción se emplea en áreas donde existe tráfico intenso debido a que esta configuración permite elegir automáticamente el mejor AP para comunicarse. En el roaming sucede algo similar, ya que puede iniciarse una sesión y continuarla mientras el usuario se mueve de una célula a otra (aunque exista un corte momentáneo en el flujo de información).

## 1.4 Topologías de las WLAN

### 1.4.1 Redes Ad Hoc o Punto a Punto

En su forma más básica, dos o más PC's que cuenten con tarjetas adaptadoras para WLAN pueden constituir una red independiente siempre y cuando se encuentren dentro de cierto rango. Este tipo de red es llamada punto a punto o *ad hoc*. Según el Estándar 802.11, ésta configuración constituye el primer tipo de BSS que el protocolo MAC admite; opera bajo demanda y no requiere administración o preconfiguración. En este caso cada usuario tendrá acceso a los recursos de otro sin la necesidad de un administrador central. En la figura 1.1 se muestra una configuración de este tipo.

### 1.4.2 Redes Tipo Infraestructura

El segundo tipo de BSS es el de infraestructura, la cual es más utilizada actualmente. Este tipo soporta la interconectividad entre una red alámbrica y una inalámbrica. Dentro de cada BSS en modo infraestructura existe un AP, que funciona como una estación central reguladora de tráfico operando en un canal determinado y ubicado en un punto fijo. La ubicación de dichos AP's se puede configurar de tal forma que las zonas de cobertura se interfieran ligeramente con el fin de proporcionar cobertura continua a las estaciones móviles.

[6] Basic Service Set
[7] Access Point


Figura 1.1
*Red Ad Hoc*

Cada AP puede suministrar servicio a muchos usuarios; el número específico depende del tamaño y de la naturaleza de la información involucrada en el proceso, así como de la configuración llevada a cabo por el administrador de Red.

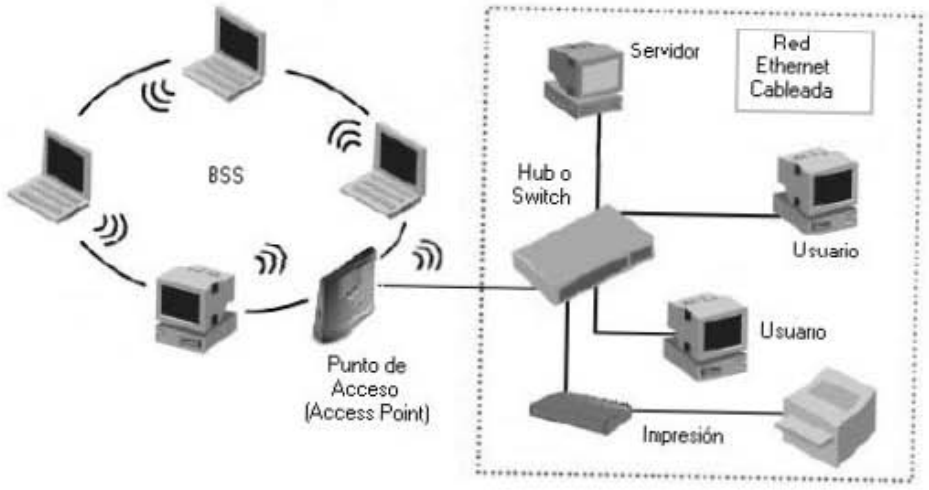



Figura 1.2
*Red Tipo Infraestructura*

Los AP tienen un rango finito de cobertura, en el orden de 152 m en interiores y 300 m en exteriores, dependiendo de las condiciones geográficas, del diseño de la red o del tipo de los equipos y su configuración.

Estos AP's pueden emplearse dentro de las WLAN's como:

1. Gateway: para tener acceso a redes externas (Internet, Intranet, etc.).
2. Bridge: para comunicarse con otros AP's con el fin de extender el área de servicio.
3. Router: para direccionar el flujo de información entrante o saliente.

Las estaciones finales o *clientes* en el modo infraestructura, establecen los enlaces en la capa MAC con los AP's. Además sólo ellos pueden comunicarse directamente con un AP determinado. Los clientes son los que realizan el proceso de búsqueda, autenticación y asociación con el fin de poder hacer uso de los servicios de la red. La búsqueda permite a los clientes descubrir los BSS disponibles dentro del área de cobertura. Los AP's envían periódicamente frames tipo *bacon* que, dentro de otras cosas, sirven a los usuarios para descubrir BSS's. Por último, es necesario lograr la autenticación del usuario para validar el acceso que le permitirá intercambiar información con el BSS.

Para resolver problemas específicos de topología, el diseñador de la red puede elegir el uso de Puntos de Extensión (EP's)[8] cuyo funcionamiento es similar al de los AP's, pero no son reconocidos por la red como tales. Como su nombre lo indica, extienden el rango de cobertura reenviando las señales de un cliente a un AP o a otro EP.

Una configuración adicional a considerar, reside en el uso antenas direccionales. Supongamos que tenemos una LAN en un edificio A y se requiere extender al edificio B, situado a más de un kilómetro de distancia. Una solución consistiría en instalar una antena en cada edificio, estando ambas en línea de vista. La antena A es conectada a la red alámbrica vía AP. La antena B es similarmente conectada a un AP en el otro edificio, el cual habilita el acceso a la red inalámbrica. Esto queda representado en la Figura 1.3.

[8] Extension Points

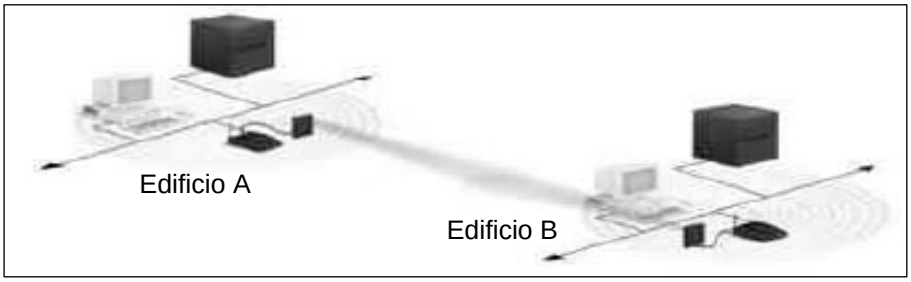



Figura 1.3
*Uso de Antenas Direccionales*

### 1.4.3 Introducción al Espectro Disperso

La mayoría de las redes WLAN utilizan la tecnología de espectro disperso, que consiste en una técnica para hacer más eficiente el ancho de banda de modo que sea más rentable, seguro e íntegro. Si el receptor no está sintonizado a la frecuencia precisa, una señal de espectro disperso parecerá ruido de fondo para dicho receptor. Existen dos técnicas de espectro disperso: saltos en frecuencia y secuencia directa.

La técnica de Saltos en Frecuencia en Espectro Disperso (FHSS)[9] emplea una portadora de banda estrecha que cambia de frecuencia de manera conocida tanto en el transmisor como en el receptor. Adecuadamente sincronizados, el objetivo es mantener un solo canal lógico. Para un receptor que no esté sintonizado, FHSS aparece como un impulso de ruido de corta duración.

La Secuencia Directa en el Espectro Disperso (DSSS) genera un patrón de bits redundantes para cada bit a transmitir. Este patrón es llamado *chip* (o código chip). Mientras más grande sea el patrón, existen mayores posibilidades de que los datos puedan ser recuperados (y por supuesto, se requeriría de más ancho de banda). Incluso si uno o más bits del chip se dañan durante la transmisión, las técnicas estadísticas contenidas en el algoritmo permitirán recobrar la información sin la necesidad de recurrir a la retransmisión. Para un receptor que no utilice esta técnica, DSSS aparece como ruido de amplio ancho de banda y de baja potencia, por lo que es ignorado por la mayoría de los receptores de banda estrecha.

[9] Esta técnica será definida en el capítulo siguiente, al igual que la DSSS

### 1.4.4 Sistemas Infrarrojos

Los sistemas infrarrojos (IR)[10] utilizan frecuencias muy altas, justo por debajo de la luz visible dentro del espectro electromagnético para transportar los datos. Tal como la luz, los IR no pueden penetrar los objetos opacos, en vez de ello se emplean técnicas como comunicación directa (línea de vista) o tecnología difusa. Estos sistemas proveen un rango bastante limitado (1 a 10 m) y típicamente se utilizan en sistemas como las PAN's[11], pero ocasionalmente se utilizan en aplicaciones específicas de WLAN. El desempeño de la tecnología IR no permite la movilidad necesaria que los usuarios requieren, por lo que sólo son empleadas en ciertas implementaciones de subredes. En el caso de WLAN IR con tecnología difusa (o reflectiva) no se requiere línea de vista, pero las células se limitan a cuartos individuales en donde sea posible la propagación de los rayos IR.

Cabe señalar que estas tecnologías son las que se especifican en el Estándar IEEE 802.11. Los estándares creados por los grupos de trabajo 802.11 a, b y g especifican diversas técnicas (estrechamente relacionadas con las anteriores) que serán tratadas con detalle en el siguiente capítulo.

### 1.4.5 Microcélulas y Roaming

Las comunicaciones inalámbricas se encuentran limitadas por el alcance que pueda tener la señal portadora para cierta potencia de transmisión. Las WLAN's utilizan células, llamadas microcélulas (similares a las de los sistemas de telefonía celular) con el propósito de extender el rango de cobertura inalámbrica. En cualquier punto, una PC equipada con un adaptador WLAN se asocia con un solo AP dentro de una microcélula. Éstas a su vez se traslapan para permitir que la comunicación sea continua. A la capacidad de los usuarios para moverse dentro de las células se le llama Roaming. El objetivo es traslapar las células de manera que el usuario no pierda conectividad y que el proceso sea invisible para el mismo.

## 1.5 Ventajas de las WLAN's

- ✓ Con una WLAN, los usuarios pueden acceder a la información compartida sin buscar un lugar donde conectarse, y los administradores de red pueden configurar a nuevos equipos sin instalar o mover cables.
- ✓ La simplicidad de instalación de una WLAN hace que ésta sea más rápida y se puede eliminar la necesidad de tender cable sobre las paredes o dentro de ellas.

[10] Infra-Red
[11] Personal Area Network

- ✓ Al implementar una WLAN, se conserva prácticamente sin cambio la estructura original del sitio donde está instalada, ya que no hay cables adicionales por muy grande que sea el número adicional de usuarios.
- ✓ En un principio los costos de la inversión inicial para una red WLAN pueden ser mayores que para una red alámbrica. Sin embargo, después de la implementación los costos de operación y mantenimiento son menores, ya que los equipos pueden moverse sin necesidad de cambiar la estructura del cable, cuestión que en muchos casos genera costos adicionales.
- ✓ La escalabilidad[12] de una red WLAN puede ser configurada en una variedad de topologías según las necesidades de las aplicaciones específicas de la red. Las configuraciones pueden ser fácilmente cambiadas de tipo punto a punto con pocas personas como usuarios, hasta una red de tipo infraestructura donde cientos de usuarios comparten los servicios de roaming en toda el área de cobertura.
- ✓ Debido a la aceptación de esta tecnología dentro del mercado, los costos de los equipos están decreciendo rápidamente, teniendo su efecto en que cada vez sea más grande el número de usuarios. Aunado a ello, se continúa con investigaciones en materia de nuevas tecnologías para lograr mayores velocidades y la compatibilidad entre distintos fabricantes.

## 1.6 Desventajas de las WLAN's

Como todo sistema de comunicaciones, existen diversos factores externos que alteran el rendimiento de las WLAN's. La interferencia y el ruido son producidos por una amplia variedad de fuentes. Por ejemplo, el medio puede estar compartido por dispositivos no deseados y que sean compatibles con el estándar 802.11 como son los PDA's[13], o bien, otros dispositivos no compatibles con dicho estándar pero que utilizan la misma frecuencia de operación, tales como teléfonos inalámbricos domésticos, hornos de microondas, transmisores de radar, etc.

La calidad de la conexión varía de manera impredecible en el espacio y tiempo, por lo que no se puede asumir una conectividad completa, es decir, a la máxima capacidad que el sistema soporta. Por ejemplo, los usuarios se mueven dentro de un lugar, abren o cierran cosas que interfieren con la señal transmitida, provocando reflexiones multitrayectoria no deseadas. Esto repercute ampliamente en la confiabilidad del enlace, que no resulta benéfico para aplicaciones que requieran un ancho de banda crítico, como lo son la voz y el video.

La libertad de movimiento tiene el inconveniente de que la confiabilidad del enlace sea variable. Cuando una estación se mueve, el enlace presentará las

[12] La escalabilidad se refiere a la posibilidad de implementar actualizaciones de hardware y software.
[13] Personal Digital Assistant

dificultades antes mencionadas y podría quedar fuera del área de cobertura. Los usuarios requieren que sus conexiones sean "parecidas", por lo que el diseño de los protocolos y de las capas físicas deben cubrir el problema de roaming y confiabilidad del enlace.

Algunas otras particularidades en el uso de radiofrcuencias o infrarrojos deben se deben tomar en cuenta. La transmisión sobre radio requiere preámbulos y encabezados en los frames para que los receptores puedan detectar la frecuencia de la portadora, el tiempo del bit y el tiempo del frame. Este tipo de tiempos no son utilizados en redes alámbricas. Físicamente, las limitaciones dependientes del hardware y el tiempo que toma la señal en llegar de una estación a otra, hace necesario el empleo de tiempos de un *buffer* (almacenamiento temporal) para que sea posible el cambio o *switching* entre la transmisión y recepción. Las diferencias entre los niveles de potencia de los transmisores y receptores hace imposible la detección de colisiones en la estación transmisora.

La seguridad representa un problema. No existen límites físicos que delimiten a la red, así que dispositivos compatibles en hardware pueden estar recibiendo información que la red transmite. Este efecto puede ser intencional o no, dado que las WLAN comparten el medio con otros dispositivos. Para solucionar esto un algoritmo llamado WEP[14] controla y encripta el tráfico, proporcionando de esta manera seguridad a la red.

## 1.7 Aplicaciones

Los espacios que considera el estándar IEEE 802.11 incluyen los interiores de construcciones tales como oficinas, instituciones financieras, tiendas y supermercados, pequeñas y medianas industrias, hospitales, hogares, entre otros. En los exteriores se consideran estacionamientos, complejos de edificios, áreas comunes, etc.

En la actualidad, una gran cantidad de oficinas están equipadas con alguna implementación alámbrica de tipo LAN. El mercado de las WLAN's será muy probablemente desarrollado en base a las soluciones inalámbricas propuestas para problemas específicos. El objetivo del mercado para las industrias que fabrican los equipos WLAN incluye aplicaciones en grandes áreas interiores, oficinas con dificultades de cableado y redes de uso temporal, entre otros. También podemos mencionar áreas donde no es factible atravesar las paredes o el techo de la construcción. Una solución podría ser el cableado bajo tierra, pero esto siempre representa un alto costo, además de que no es sencillo reubicar una instalación de este tipo.

[14] Wired Equivalent Privacy

Otra aplicación muy importante se sitúa en edificios de valor histórico, pues es preciso no dañar la estructura original del inmueble. Un ejemplo más, es aplicado en las bibliotecas, donde sería costoso establecer una terminal para cada usuario: el problema quedaría resuelto con una WLAN. Por último mencionamos aplicaciones temporales, como en el caso de las campañas políticas, donde se requiere hacer un uso temporal de las instalaciones así como del equipo. La ventaja de una WLAN para esta aplicación es que el equipo es totalmente reutilizable y no se necesita planear una infraestructura que después tenga que ser removida.

## 1.8 Consideraciones Previas a la Elección de una Solución WLAN

¿Por qué un usuario debe considerar el uso de una WLAN? Obviamente, ésta es una pregunta que cada individuo interesado en emplear esta tecnología debe formularse antes de tomar una decisión hacia el siguiente paso, que es el diseño de la solución para un problema específico. Hasta hace poco, las redes LAN constituían la única opción disponible para proporcionar la conectividad necesaria entre varios usuarios dentro de un ambiente *dinámico*. Los costos del cableado así como su planeación, eran tediosos y en ocasiones la pesadilla de los administradores de una red LAN (en algunos casos sigue siéndolo). Muchos de estos problemas ya pueden ser solucionados gracias a la tecnología WLAN.

Las WLAN's ampliarán los arreglos cableados, proporcionando flexibilidad y movilidad para el futuro. Los críticos han argumentado que las soluciones inalámbricas resultan más costosas comparadas con las soluciones que brindan los sistemas LAN tradicionales. Aunque esta aseveración es cierta en un nivel superficial, esta tendencia está cambiando rápidamente. Los proveedores de equipos inalámbricos han reducido los costos de dichos equipos, además de haber mejorado la velocidad y el desempeño de los sistemas.

La comparación de las tecnologías LAN vs. WLAN, no implica que una desplazará a la otra. En vez de eso, el diseño debe buscar y aplicar distintas soluciones para problemas específicos. Además, la capacidad de implementar y mezclar servicios y tecnologías sigue siendo la mejor opción. Ningún servicio puede desplazar totalmente a otro cuando los sistemas pueden coexistir armoniosamente dentro de un entorno que crece rápidamente y demanda flexibilidad. El uso de soluciones inalámbricas puede ser una extensión de una tecnología, en vez de ser el desplazamiento de otra.

La siguiente tabla resume posibles planteamientos y aplicaciones que darán significado a un proyecto piloto a gran escala de una implementación WLAN. No considera todos los planteamientos existentes, pero expone algunos criterios para

el proceso de evaluación y contribuye a la justificación del proyecto. Dichas discusiones son únicamente lo que *podría ser*, más no lo que *debe ser*.

En relación a este proyecto de tesis, en la tabla 1.1 se marcan con un punto los planteamientos que son válidas para este estudio.

| PLANTEAMIENTO | SÍ | NO |
|---|---|---|
| ¿La tecnología a implementar es capaz de ser manejada por servicios existentes, tales como sistemas alámbricos? | • | |
| ¿Es nueva esta tecnología en la organización? | • | |
| ¿Existen otras opciones que puedan ser estudiadas? | • | |
| ¿Existen otras instituciones utilizando este servicio? | • | |
| Si existen otras instituciones usando el servicio, ¿es favorable la instalación del servicio así como su operación? | • | |
| ¿Existen estándares en la industria para este servicio? | • | |
| Si los estándares no existen, ¿hay otros estándares que estén siendo empleados por otros proveedores? | | • |
| ¿La solución técnica propuesta puede compararse favorablemente con otras? | • | |
| ¿Se comprenden claramente los requerimientos físicos y eléctricos de este servicio? | • | |
| ¿Los proveedores muestran un amplio conocimiento de la tecnología así como sus aplicaciones para la solución propuesta? | • | |
| ¿Es la única opción disponible para resolver las necesidades de la institución? | | • |
| Si es la única solución, ¿es ésta la más costosa para instalar y operar que el sistema actual? | • | |

Tabla 1.1
*Planteamientos acerca de una solución WLAN*

Obviamente, estos criterios deben ser reemplazados o modificados de acuerdo con necesidades específicas de cada institución. Si se propone un punto por cada respuesta afirmativa y cero para las respuestas negativas, podremos definir si seguimos adelante con el proyecto u optamos por investigar más a fondo diferentes opciones de acuerdo al siguiente criterio: si se obtiene una puntuación menor a 10 unidades, sería conveniente revisar exhaustivamente otras tecnologías antes de optar por un sistema WLAN. Si se obtienen diez puntos o más (en este caso tenemos 10), podemos afirmar que se está tomando una buena decisión al optar por un sistema WLAN.

Por último, en la tabla 1.3 se listan algunos aspectos de los sistemas alámbricos e inalámbricos con el propósito de poder elegir con mayor claridad la solución a un problema determinado.

| SISTEMA ALÁMBRICO | SISTEMA INALÁMBRICO |
|---|---|
| El presupuesto es importante, y los costos para la instalación de la red son relativamente bajos | El presupuesto no es importante. |
| La ubicación de la red será fija, los usuarios jamás serán reubicados. | La ubicación de la red será temporal, o los usuarios estarán continuamente en movimiento o se incorporarán más usuarios. |
| Los conductos por donde pasará el cable se encuentran vacíos o será sencillo tender el cable a través de ellos. | No existen conductos adecuados para tender una red de cable o sería costoso crear nuevos conductos. |
| No existen requisitos o restricciones legales respecto a la instalación de cables. | El lugar de la instalación requiere tipos especiales de cable que son muy costosos, o que no pueden ser tendidos por falta de espacio. Existen algunas restricciones en cierto tipo de construcciones por razones de seguridad. |
| La apariencia no es importante. Las paredes son fáciles de modificar y no se ve afectada la estética del recinto. | Existen ciertas construcciones en las que no es factible tender una red cableada, como en edificios históricos y en aquellos lugares donde se afecte la apariencia visual de la construcción, como en oficinas de cristal, por ejemplo. |

Tabla 1.2
*Comparación entre las Soluciones Alámbricas e Inalámbricas*

Con base en las conjeturas anteriores, se procederá a elaborar la propuesta para ampliar el servicio de red a la comunidad de la Facultad de Ingeniería mediante una solución WLAN.

CAPÍTULO DOS

# Tecnologías de Modulación Empleadas en las WLAN's

## 2.1 Introducción

Para cualquier implementación de un sistema de radiocomunicaciones, la selección de una técnica de modulación en particular involucra una serie de consideraciones generales que deben ser tomadas en cuenta. Como ejemplo citamos las siguientes:

- Maximizar la eficiencia espectral (bits/Hz)
- Minimizar la potencia requerida
- Maximizar la utilización del sistema[1]
- Minimizar el costo del sistema.

De acuerdo a lo anterior, la radio tecnología en la cual las WLAN's están basadas se conoce como modulación de Espectro Disperso (SS)[2]. Esta tecnología fue muy utilizada para las comunicaciones militares en décadas pasadas, debido a su resistencia a la interferencia, a los efectos causados por las multitrayectorias y a la atenuación de la señal, entre otras características. Como resultado, los sistemas basados en SS pueden coexistir con otros sistemas de radiocomunicaciones sin que se causen obstrucciones entre ellos.

El efecto inmediato de este comportamiento es que los sistemas basados en SS pueden operar sin la necesidad de licitarlas, y eso hace que la modulación en SS sea la tecnología adecuada para la implementación de las WLAN libres de licencia y los servicios de banda ancha.

## 2.2 Definición de Espectro Disperso

Las técnicas de modulación en espectro disperso se definen como aquéllas técnicas en las cuales:

- El ancho de banda de la señal transmitida es mucho más grande que el ancho de banda del mensaje original, y

[1] Por utilización del sistema entendemos que el ancho de banda designado para cierta aplicación sea aprovechado en su totalidad y con mínima interferencia con los canales adyacentes
[2] Spread Spectrum

- El ancho de banda de la señal transmitida está determinado por el mensaje a ser transmitido y por una señal adicional conocida como el Código de Dispersión (SC)[3].

Dado que la energía del mensaje se distribuye en un ancho de banda mucho más grande que el mínimo que se requiere, las técnicas de modulación en SS tienen dos ventajas importantes: baja densidad de potencia y redundancia.

La baja densidad de potencia se refiere al hecho de que la energía transmitida se dispersa sobre una banda ancha y por tanto, la cantidad de energía para una frecuencia específica es muy baja. El efecto de la baja densidad de potencia de una señal transmitida es tal, que no interferirá la actividad de otros sistemas receptores en la misma área, y por otra parte, no será fácilmente detectada por intrusos, proporcionando de esta manera un cierto nivel de seguridad intrínseca.

La redundancia se refiere al hecho de que el mensaje es (o puede ser) presentado en diferentes frecuencias de donde podría ser recuperado en caso de errores. El efecto de la redundancia en los sistemas basados en SS es que presentan alta resistencia al ruido y a la interferencia, siendo capaces de recuperar los mensajes incluso si el ruido está presente en el medio.

En resumen, las principales ventajas de las transmisiones en SS son las siguientes:

- Las señales en SS pueden ser utilizadas donde otros sistemas de radiofrecuencia se encuentren operando, con un mínimo impacto en el desempeño de ambos sistemas.
- Las características anti-mutitrayectoria de la transmisión y recepción utilizando técnicas de SS son atractivas en aplicaciones donde las multitrayectorias sean altamente probables.
- Las características anti-interferencia son importantes en algunas aplicaciones, por ejemplo, en redes que operan en lugares de manufactura donde la interferencia podría causar graves problemas.
- La conveniencia en el uso de bandas sin licencia (ICM) resulta atractiva para los proveedores de equipo así como para los consumidores. La operación de sistemas en estas bandas de frecuencia están definidas en el Estándar 802.11.

## 2.3 Principios de Operación de los Sistemas Basados en SS

Las técnicas de modulación en Espectro Disperso se componen de dos procesos de modulación consecutiva que generan la ampliación del ancho de banda de la señal transmitida.

[3] Spreading Code

- Proceso 1**:** Ejecutado en el Código de Dispersión. Éste es el proceso mediante el cual se genera la amplitud del ancho de banda de la señal transmitida.

- Proceso 2**:** Ejecutado por el mensaje a ser transmitido. Se emplea una modulación convencional para transmitir el mensaje.

En base a esto se definen dos técnicas de modulación en SS: Secuencia Directa (DS)[4] y Saltos en Frecuencia (FH)[5].

Antes de analizar con detalle estas dos técnicas, es preciso mencionar algunas de las herramientas que han sido desarrolladas con el propósito de hacer más rápidos y eficientes a estos sistemas.

### 2.3.1 Secuencias Pseudo – Aleatorias

Una secuencia de Pseudo-Ruido (PN)[6] o *pseudo-aleatoria* se define como una secuencia codificada de ceros y unos que tienen ciertas propiedades de autocorrelación. La clase de secuencias utilizadas en las comunicaciones en SS son usualmente *periódicas* de manera que los 1's y los 0's se repiten exactamente con un periodo conocido.

El nombre de secuencias PN reside en que la secuencia actúa como un ruido en la portadora (aunque de manera determinística) que es utilizado para dispersar la energía de la señal. También se llama secuencia pseudo-aleatoria porque la secuencia de 1's y 0's no es una secuencia totalmente aleatoria (debido a su periodicidad) aunque para el usuario pareciera serlo. Además, las secuencias aleatorias no son predecibles.

Las secuencias PN cuentan con las siguientes propiedades:

Balance

En cada periodo de la secuencia, el número de 1's binarios difiere del número de ceros en un dígito.

$$PN = +1\ +1\ +1\ -1\ +1\ -1\ -1 \rightarrow \sum = +1$$

Cuando se modula una portadora con una secuencia PN, el balance entre unos y ceros (componente de DC) puede limitar el grado de supresión de la portadora, debido a que la supresión de la portadora depende de la simetría de la señal moduladora.

[4] Direct Sequence
[5] Frequency Hopping
[6] Pseudo Noise Sequence

Run-lenght (*Secuencia*)

Dentro de la secuencia de 1's y 0's en cada periodo de una secuencia de longitud máxima, una mitad de la secuencia tiene longitud uno (un elemento), una cuarta parte tiene longitud dos (dos elementos), una octava parte tiene longitud tres y así sucesivamente hasta que esas fracciones representen algún significado en la secuencia. Esta propiedad es llamada *secuencia* (run-lenght).

Autocorrelación

El origen del nombre *pseudo-noise* se debe a que la señal digital tiene una función de autocorrelación muy similar a la que posee el ruido blanco: impulsos. La función de autocorrelación para la secuencia *periódica* se define como el número de coincidencias menos las diferencias que existen en la comparación término a término en un periodo completo de la secuencia.

Para ejemplificar estas propiedades veamos el siguiente ejemplo de una secuencia de salida en términos binarios:

$$C_n = 0011101$$

Y en términos de niveles -1 y +1 la secuencia está dada por:

$$C_n = -1, -1, +1, +1, +1, -1, +1$$

Para esta secuencia, vemos que hay tres –1 y cuatro +1 en un periodo de la secuencia, lo cual satisface la propiedad de Balance.

Para N = 7, hay un total de cuatro *secuencias* (de 1's y 0's) en un periodo de la secuencia ejemplo. Leyendo la secuencia binaria de derecha a izquierda, hay cuatro secuencias distinguibles: 00, 111, 0 y 1. Dos de las secuencias (la mitad del total) son de longitud uno, y una secuencia (un cuarto del total) es de longitud dos, lo que satisface la propiedad de la Secuencia.

En la Fig. 2.1a se muestran dos periodos completos de una secuencia. La Fig. 2.1b muestra la función de autocorrelación $R_C(\tau)$ graficada como una función del tiempo ($\tau$). En esta figura, el parámetro $T_C$ denota la duración de un símbolo binario 1 ó 0 en la secuencia, y *N* es la longitud de un periodo de la secuencia. Entonces es claro que se satisface la propiedad de Autocorrelación.

.

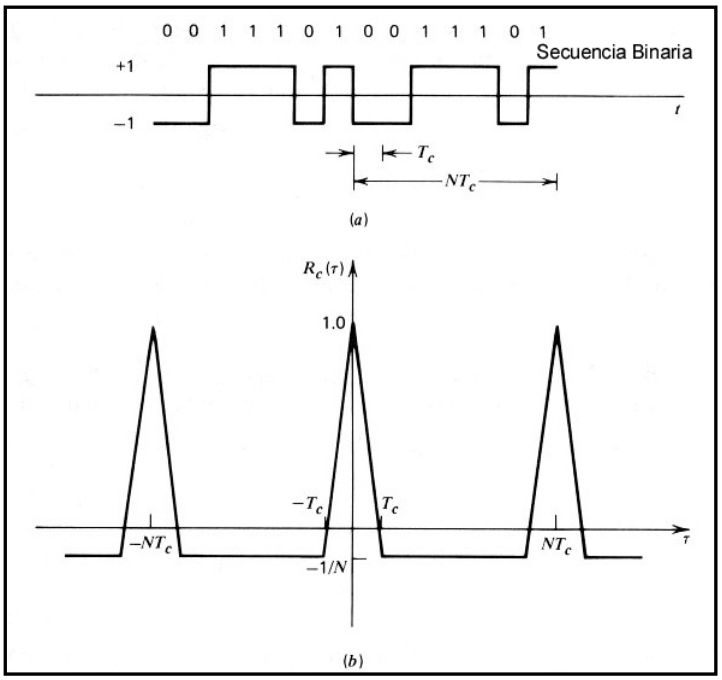



Figura 2.1
*a) Secuencia Pseudo-aleatoria*
*b) Gráfica del espectro de la secuencia Pseudo-aleatoria*

### 2.3.2 Secuencia PN Barker

El código Barker es utilizado como secuencia pseudo-aleatoria en el proceso de *chipping*[7], mediante el cual se obtiene una señal en SS. Este código de longitud de 11 bits se utiliza para lograr la dispersión del espectro. El proceso consiste en realizar una función XOR entre los bits a transmitir y una secuencia pseudo-aleatoria Barker de 11 bits de longitud. Este código cambia de fase seis veces para un solo símbolo lo que significa que la portadora también cambia de fase seis veces para cada símbolo codificado.

La función XOR (Tabla 2.1) lleva a cabo lo que se denomina *adición módulo – 2* en la secuencia de datos digitales. Recordemos la tabla de verdad para una función XOR:

| a | b | f (a,b) |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Tabla 2.1
*Tabla de Verdad XOR*

[7] Se refiere al proceso de agregar el Código de Dispersión.

El efecto de la adición módulo – 2 consiste en la inversión del código PN en cada transición (cambios de nivel) de la secuencia de los datos y por otra parte, dispersar el ancho de banda.

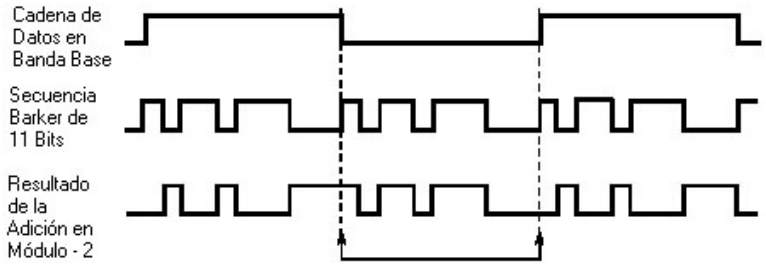



Figura 2.2
*Efecto de la Adición Módulo – 2*

En el receptor, la señal recibida es demodulada y se procesa de forma digital para realizar el proceso inverso a la dispersión de la señal. Este proceso consiste en una correlación con la secuencia Barker de 11 bits. Los registros del sistema almacenan la secuencia Barker. Si esta secuencia está codificada con 1 y –1, los productos del proceso de correlación se reducen a simples sumas y restas. El resultado de este proceso es una serie de "picos" positivos y negativos que coinciden con los 1's y 0's emitidos.

Los códigos Barker son conocidos por poseer buenas propiedades de correlación aperiódica, lo que significa que debido al comportamiento no periódico del código, un filtro capaz de correlacionar la señal recibida, podrá fácilmente identificar la ubicación de la secuencia de bits.

## 2.4 Secuencia Directa

La técnica de Secuencia Directa (DSSS)[8] está definida en el Estándar 802.11 en la banda de 2.4# GHz y opera en una de las 16 portadoras dentro de ese rango de frecuencias (las bandas específicas para cada país son diferentes, según los grupos de trabajo 802.11 y 802.11 d). La portadora seleccionada estará modulada en PSK[9] con un ancho de banda de 22 MHz con tasas de transmisión de 1 y 2 Mbps. En el grupo 802.11 b se agregan tasas de transmisión de 5.5 Mbps y 11 Mbps (en la banda de 2.4 GHz) manteniendo el ancho de banda de 22 MHz.

De acuerdo a los principios de operación de los sistemas SS, dentro del primer proceso, la señal portadora es modulada durante el transcurso de cada bit del

[8] Direct Sequence Spread Spectrum
[9] Phase Shift Key

mensaje, siguiendo una secuencia de bits específica, conocida como *chip*. El proceso es en conjunto es conocido como *chipping* y da como resultado la sustitución de cada bit del mensaje por (la misma) secuencia de chips. Entonces, en los sistemas DSSS, el Código de Dispersión está dado por la secuencia de chips utilizados para representar los bits del mensaje.

Durante el segundo proceso se realiza la modulación del mensaje. Por efecto de la *adición módulo 2* de la cadena de datos con la secuencia Barker, los ceros del mensaje son sustituidos por la misma secuencia de chips; los unos del mensaje, son sustituidos por la misma secuencia pero de manera invertida. De esta forma, los bits "0" y "1" del mensaje son representados por diferentes secuencias de chips, siendo unos bits la versión invertida de los otros, como se ilustró en la Figura 2.2.

En el receptor, la señal recibida es sometida a un proceso de demodulación para recobrar la señal y posteriormente esta señal de espectro disperso es procesada para recuperar el mensaje original mediante un proceso llamado *dispreading*, donde se regresa la señal a su ancho de banda original. La siguiente figura muestra este proceso (Fig. 2.3).

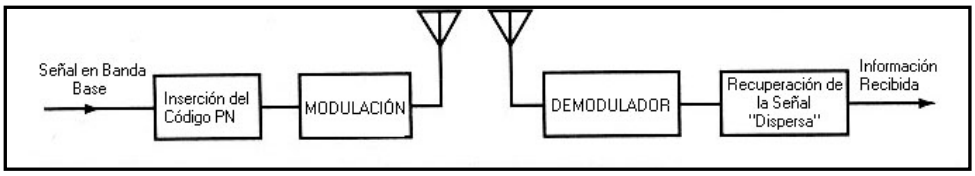



Figura 2.3
*Demodulación de una Señal DSSS*

La Fig. 2.4 proporciona un ejemplo simple que describe el proceso de dispersión de la señal en un sistema DSSS. Un pulso cuadrado con duración Tb representa un dígito de información binaria en el dominio del tiempo, y su transformada de Fourier es un pulso *Sinc* con cruces en cero en espaciados por 1/Tb. La señal de información es multiplicada por una secuencia de pulsos de menor ancho con duración de Tc y cruces con cero espaciados por 1/Tc para formar de esta manera, la señal en espectro disperso. Los pulsos de menor ancho (chips) tienen una amplitud de ± 1. El factor de expansión del ancho de banda (factor de dispersión) está dado por N = Tb / Tc; la tasa de transmisión en baudios es Rb = 1 / Tb y la tasa de transmisión de los chips del sistema es Rc = 1 / Tc. Dado que la potencia transmitida se dispersa a través del ancho de banda disponible, ésta es N veces más baja que en una transmisión sin utilizar la dispersión del espectro. Las amplitudes de los chips están codificadas en un patrón de aparición periódica y aleatoria

conocido como *spreading code*. Idealmente, el SC está diseñado de tal manera que las amplitudes de los chips son estadísticamente independientes los unos de los otros.

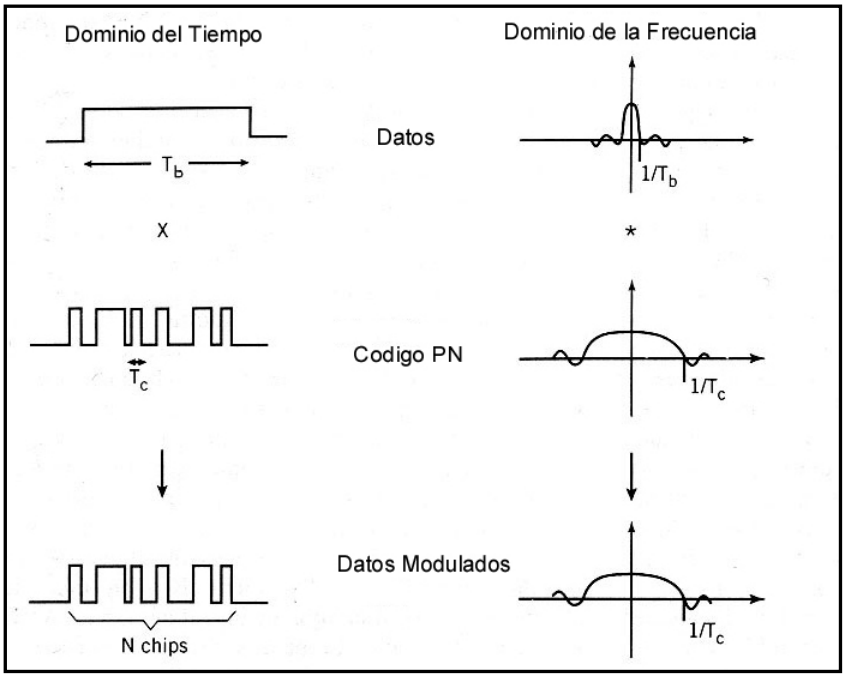



Figura 2.4
*Dispersión de una Señal Binaria*

### 2.4.1 Ganancia de Proceso

El efecto de la codificación de la señal mediante el esquema DSSS produce que el ancho de banda se vea incrementado considerablemente. Una regla general para los sistemas DSSS es que el ancho de banda de la señal en SS es dos veces el "chip rate", esto significa que si se utiliza un código Barker de 11 bits de longitud con un chip rate de 11 Mchips/s, entonces el ancho de banda que ocupará la señal DSSS será de 22 MHz. Esto es permisible para tres canales independientes sin traslaparse dentro de la banda de frecuencias ICM.
En el receptor la señal en SS es de nuevo sometida a un proceso de *adición módulo 2* empleando una secuencia PN. Este procedimiento resulta en la recuperación de la señal en su ancho de banda original y elimina cualquier ruido o señal de interferencia. Un filtro paso banda también puede rechazar señales indeseables y la potencia del ruido. En este mecanismo de dispersión/recuperación se obtiene una figura de mérito conocida como *Ganancia de Proceso*. La ganancia de proceso está dada por la siguiente ecuación:

$$Gp = \frac{BW_{(SS)}}{R_{(INFO)}}$$

Donde:

| | |
|---|---|
| **Gp** | Ganancia de Proceso |
| **BW**$_{SS}$ | Es el ancho de banda de la señal después del proceso de dispersión |
| **R**$_{(INFO)}$ | Es la tasa de transmisión de la señal en banda base |

Otra forma de definirlo es de la siguiente manera: La ganancia de proceso es la cantidad en la cual se ve mejorado el desempeño del sistema a través del uso de la técnica en espectro disperso, en otras palabras, es la diferencia entre el desempeño del sistema empleando técnicas de espectro disperso y el desempeño del sistema sin el uso de dichas técnicas. Por ejemplo, si el sistema opera en la modalidad DSSS a 2 Mbps, la ganancia de proceso será:

$$Gp = 10\log\frac{22MHz}{2Mbps} = 10.4dB$$

## 2.5 Saltos en Frecuencia

Esta técnica de modulación de Saltos en Frecuencia (FHSS)[10] está definida en el grupo de trabajo 802.11 y opera en la banda de 2.4 GHz, utilizando 79 frecuencias que van desde 2.400 GHz a 2.480 GHZ (dependiendo de las especificaciones de cada país, definidas en el grupo de trabajo 802.11 d). Cada una de estas frecuencias están moduladas en GFSK[11], con un ancho de banda de 1 MHz.

La técnica de saltos en frecuencia también puede ser descrita como una técnica de modulación de dos etapas o procesos.

- Proceso 1. La frecuencia de la portadora es periódicamente modificada (en forma de saltos) siguiendo una secuencia específica de frecuencias. En los sistemas FHSS, el código de dispersión consiste en una lista de frecuencias utilizadas para la señal portadora.

- Proceso 2. El mensaje modula a la señal portadora (FSK) generando una señal de banda estrecha con una duración igual a la de cada salto; a pesar de ello se está produciendo una señal de banda ancha debido a que el ancho de banda total es ocupado por cada una de las señales antes mencionadas.

La primera etapa puede ser cualquier técnica de modulación digital estándar, mientras que la segunda etapa es una modulación M-FSK. La señal modulada digitalmente hace una selección de una de las M frecuencias para utilizarla como la

[10] Frequency Hopping Spread Spectrum
[11] Gaussian Frequency Shift Key. Ésta técnica se estudiará en el capítulo siguiente.

frecuencia de la portadora. En otras palabras, la frecuencia portadora de los datos modulados digitalmente es modificada a lo largo de un amplio rango de frecuencias prescritas por un código PN periódico. Las modificaciones en las frecuencias de la portadora producen la extensión deseada del espectro de la señal transmitida. Estos cambios no afectan el desempeño del sistema ya que este proceso no agrega ruido; entonces el desempeño del sistema respecto al ruido es el mismo que si dicho sistema trabajara únicamente con la señal modulada digitalmente.

Tal y como los sistemas SS, la técnica FHSS permite la coexistencia de muchos sistemas operando con códigos ortogonales en la misma banda de frecuencias, además de proporcionar un cierto grado de privacidad al utilizar una señal por usuario, asociando a cada usuario un patrón aleatorio de frecuencias.

Una diferencia entre los dos métodos de dispersión del espectro es que la técnica DSSS utiliza el ancho de banda total del sistema durante todo el tiempo de transmisión, mientras que la técnica FHSS utiliza sólo una porción del ancho de banda disponible en cierto instante de tiempo.

En las siguientes figuras se muestran los diagramas de bloques de un transmisor y receptor típicos para un sistema FHSS.

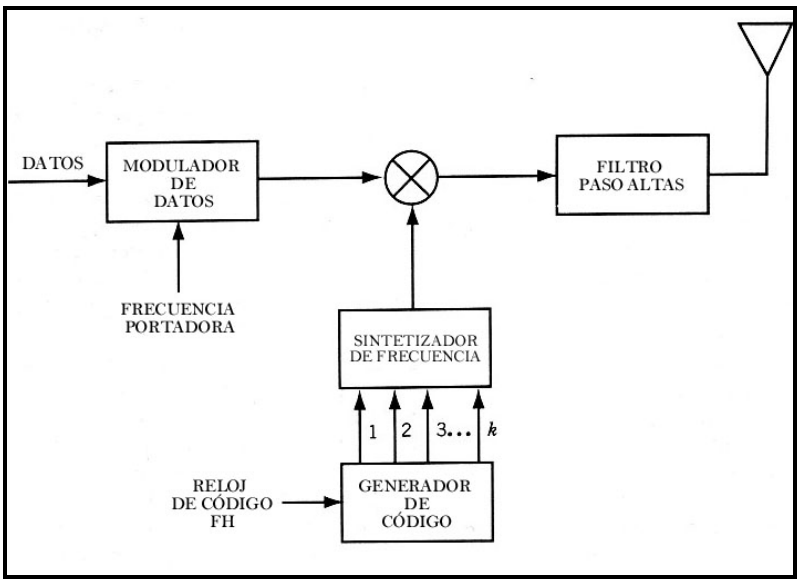



Figura 2.5
*Diagrama de Bloques de un Transmisor FHSS*

En el transmisor, la modulación digital y la modulación sobre los saltos en las frecuencias son implementadas en dos etapas. Los saltos en frecuencia son seleccionados aleatoriamente usando un sintetizador de frecuencia controlado por el generador de código PN. Un filtro de amplio ancho de banda es aplicado a la señal para delimitar el espectro antes de que la señal alimente a la antena.

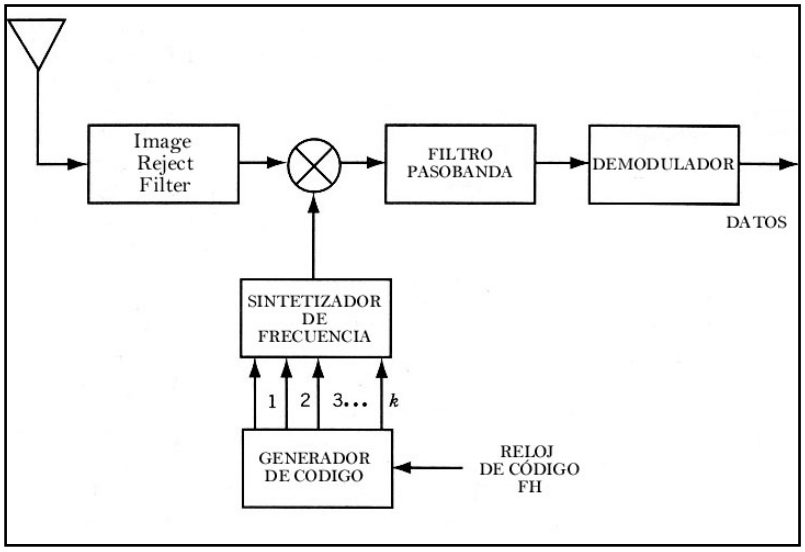



Figura 2.6
*Diagrama de Bloques de un Receptor FHSS*

El receptor cuenta con un filtro que es capaz de captar todo el ancho de banda de la señal. Este filtro está seguido de un sintetizador de frecuencia controlado por el código PN y sincronizado con el sintetizador del transmisor. Después de la etapa en que la señal es demodulada en frecuencia, la señal es procesada a través de un filtro paso banda con reducción de ruido, cuyo ancho de banda es el mismo que el de los símbolos de información transmitidos. La etapa final del receptor es el demodulador de los datos, el cual demodula la primera etapa de la modulación digital.

En un sistema FHSS, el intervalo de tiempo que ocupa cada salto en frecuencia es denominado duración del chip. En contraste con un sistema DSSS, la duración del chip en un sistema FHSS no está determinado por el valor recíproco del ancho de banda, sino que forma parte de un parámetro de diseño independiente. Esto se debe a que el sistema no utiliza un solo salto por símbolo de información, o más bien por bit. Si la duración del chip es menor que la duración del bit, entonces tendremos más de un salto por bit; a este tipo de sistema se le denomina como sistema *fast-FHSS*. Si la duración del chip es mas grande que la del intervalo de duración del bit, tendremos más de un bit por salto; a este tipo de sistemas se le denomina sistema *slow-FHSS*.

La técnica de saltos en frecuencia es efectiva para combatir la interferencia producida por equipos de transmisión en banda estrecha y de frecuencia selectiva.

## 2.6 Codificación Diferencial

El Estándar 802.11b especifica la modulación diferencial PSK (DPSK)[12] en los sistemas basados en DSSS con tasas de transmisión mayores a 2 Mbps. En este tipo de modulación, los datos en banda base son diferencialmente codificados en la transmisión para una subsecuente demodulación por un decodificador diferencial en el receptor. Con una modulación DPSK, la información está contenida por la diferencia de fase entre los elementos adyacentes de la señal transmitida, esto es, la presencia de un cero o un uno binario se manifiesta por la similitud o la diferencia de símbolo cuando es comparado con el símbolo precedente. Por tanto, no es necesario que el receptor cuente con una referencia de fase coherente en el demodulador para recuperar la señal. Sin embargo, a cambio de la simplicidad de este sistema se necesita un alto BER[13] (Tasa de Bits Erróneos) para una cierta SNR[14] (Relación Señal / Ruido), pues el ruido perturba a la fase de referencia y por ende a la información de la señal.

### 2.6.1 CCK

En el Estándar 802.11b se especifica este esquema de modulación para tasas de transmisión a 5.5 y 11 Mbps en la banda de 2.4 GHz. CCK (Complementary Code Keying) se basa en el uso de secuencias complementarias. Una secuencia binaria complementaria es un subconjunto de una clase más general de códigos conocidos como códigos polifásicos. La modulación en CCK utiliza estos códigos polifásicos complementarios.

Los códigos complementarios utilizados en el Estándar IEEE 802.11 tienen una longitud de código de 8 bits y una tasa de transmisión de *chips* de 11 Mchips/s. Los 8 chips complejos comprenden un solo símbolo. Haciendo la tasa de transmisión a 1.375 Msímbolos/s, los 11 Mbps de la forma de onda terminan por ocupar el mismo ancho de banda que los 2 Mbps alcanzados por la modulación QPSK descrita en el Estándar 802.11 y permitiendo 3 canales simultáneos sin interferencia en la banda de frecuencias ICM a 2.4 GHz. Los 8 bits del código CCK se derivan de la siguiente fórmula:

$$C = \left\{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, \right.$$
$$\left. e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \right\}$$

donde C es la palabra del código con el bit menos significativo al inicio y el bit más significativo al final. Esta extraña fórmula es utilizada para generar el conjunto de

[12] Differential Phase Shift Keying
[13] Bit Error Rate
[14] Signal to Noise Ratio

códigos que permitirán la transmisión a 5.5 y 11 Mbps. Los parámetros $\varphi_1$ - $\varphi_4$ determinan los valores de la fase para el conjunto de los códigos complejos. Para 11 Mbps cada símbolo representa 8 bits de información. A 5.5 Mbps se transmiten 4 bits por símbolo. A continuación se describirá el proceso que se lleva a cabo para lograr una tasa de transmisión de 11 Mbps. Para lograr la codificación, una trama de datos es alimentada a un procesador de banda base. Esta trama se particiona en bytes (d7, d6, d5…d0) donde d0 es el bit menos significativo. Los 8 bits son agrupados en pares de bits, llamados *dibits* y son utilizados para codificar los parámetros de fase $\varphi_1$ - $\varphi_4$ de acuerdo al esquema mostrado en la tabla 2.2.

Tabla 2.2
*Dibits y Parámetros de Fase*

| Dibit | Parámetro de Fase |
|---|---|
| (d1, d0) | $\varphi_1$ |
| (d3, d2) | $\varphi_2$ |
| (d5, d4) | $\varphi_3$ |
| (d7, d6) | $\varphi_4$ |

Después, la codificación se basa en la modulación DQPSK como se especifica en la siguiente tabla.

Tabla 2.3
*Asignación de Fase*

| Dibit $(d_{i+1}, d_i)$ | Fase |
|---|---|
| 00 | 0 |
| 01 | $\pi$ |
| 10 | $\pi/2$ |
| 11 | $-\pi/2$ |

Veamos ahora un ejemplo de cómo una palabra de código es generada.

Tomando una trama de bits dada por d7, d6, d5, ... , d0 = 1 0 1 1 0 1 0 1. Entonces, de la tabla anterior tenemos:

d1, d0 = 01, entonces $\varphi_1 = \pi$
d3, d2 = 01, entonces $\varphi_2 = \pi$
d5, d4 = 11, entonces $\varphi_3 = -\pi/2$
d7, d6 = 10, entonces $\varphi_4 = \pi/2$

Sustituyendo estos parámetros de fase en la fórmula:

$$C = \left\{ \begin{matrix} e^{j(\pi+\pi-\pi/2+\pi/2)}, e^{j(\pi-\pi/2+\pi)}, e^{j(\pi+\pi+\pi/2)}, -e^{j(\pi+\pi/2)}, e^{j(\pi+\pi-\pi/2)}, \\ e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, e^{j(\pi)} \end{matrix} \right\}$$

$$C = \left\{ e^{j2\pi}, e^{j\pi}, e^{j\frac{5}{2}\pi}, -e^{j\frac{3}{2}\pi}, e^{j\frac{3}{2}\pi}, e^{j\pi/2}, -e^{j2\pi}, e^{j\pi} \right\}$$

Por la fórmula de Euler tenemos:

$$e^{j\theta} = \cos\theta + j\sin\theta$$

$$C = \left\{ \begin{array}{l} \cos 2\pi + j\sin 2\pi, \cos\pi + j\sin\pi, \cos\frac{5\pi}{2} + j\sin\frac{5\pi}{2}, -\cos\frac{3\pi}{2} - j\sin\frac{3\pi}{2}, \cos\frac{3\pi}{2} + j\sin\frac{3\pi}{2}, \\ \cos\frac{\pi}{2} + j\sin\frac{\pi}{2}, -\cos 2\pi - j\sin 2\pi, \cos\pi + j\sin\pi \end{array} \right\}$$

Por último, la palabra de código esta dada por:

$$C = \{1, -1, j, j, -j, j, -1, -1\}$$

En la Fig. 2.7 se muestra el diagrama de bloques de un transmisor CCK donde se puede apreciar cómo son empleadas las palabras código (o códigos complejos).

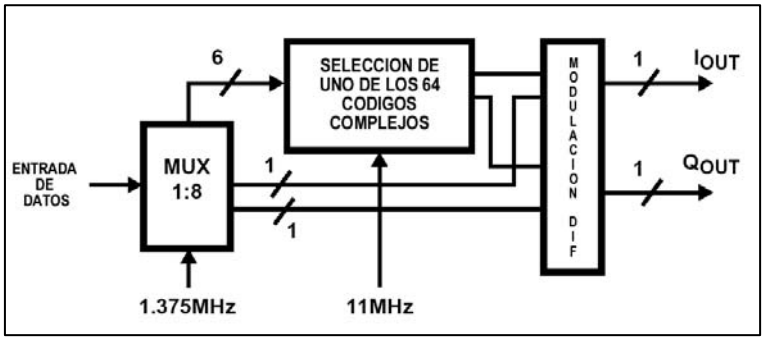



Figura 2.7
*Esquema de Modulación CCK*

De forma más general, la modulación en CCK puede representarse en el siguiente diagrama de bloques:

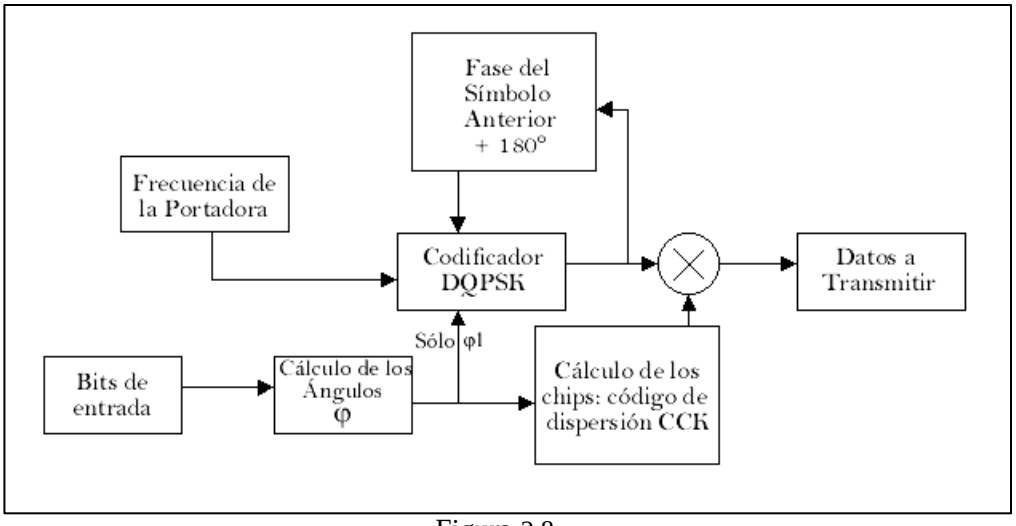



Figura 2.8
*Esquema General de Modulación CCK*

### 2.6.2 PBCC

El Estándar IEEE 802.11 también soporta una técnica opcional conocida como Packet Binary Convolutional Coding (PBCC) para alcanzar tasas de transmisión de 5.5 y 11 Mbps. Esta técnica de modulación utiliza un codificador convolucional que trabaja a la mitad de la tasa de transmisión empleada y por definición, genera dos bits de salida por cada bit de entrada. Los bits de salida del decodificador son *mapeados* en una constelación DQPSK para el caso de 11 Mbps y en una constelación DBPSK para una tasa de transmisión de 5.5 Mbps. Para suministrar una secuencia pseudo–aleatoria a esta técnica, se emplea un código pseudo–aleatorio de cobertura para variar la constelación DQPSK o DBPSK. En la siguiente figura se emplea un diagrama de bloques para ilustrar lo anterior:

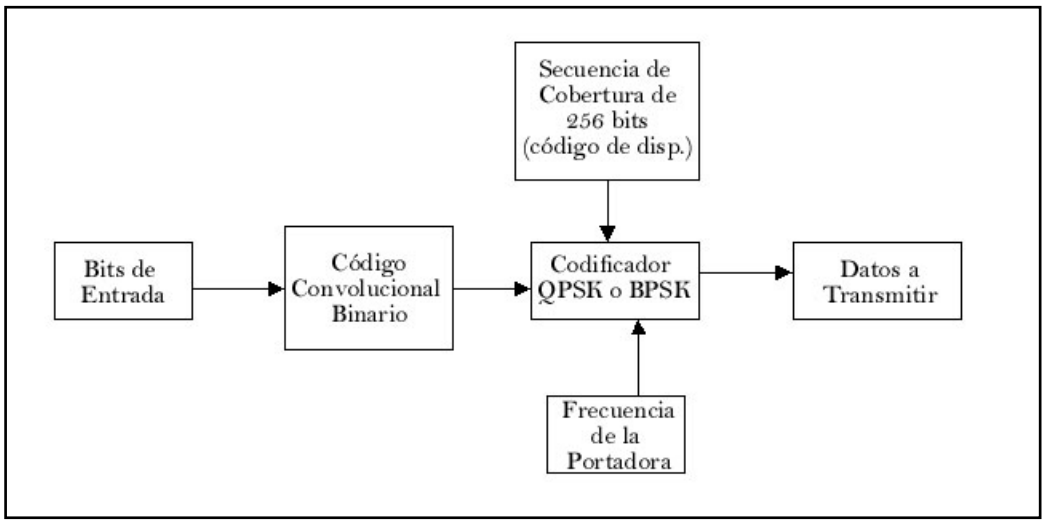



Figura 2.9
*Esquema General de Modulación PBCC*

Una secuencia de cobertura de 256 bits es utilizada para variar la constelación DQPSK o DBPSK. La secuencia de cobertura es generada tomando una secuencia de 16 bits: 0011 0011 1000 1011 y rotando posteriormente 3 bits hacia la izquierda; esto durante 15 veces para generar una trama de 16 secuencias que contienen 16 bits cada una. Esta secuencia de 256 bits es utilizada repetidamente para variar la constelación utilizada para transmitir cada chip. Específicamente, si se codifica un cero binario, entonces se utilizará una constelación; si se codifica un uno binario, la constelación es rotada $\pi/2$.

Es importante notar que en esta técnica no se menciona la dispersión del espectro. En vez de ello, los datos son codificados directamente en la tasa de transmisión deseada (11Mbps o 5.5 Mbps). Sin embargo, el uso de una secuencia de cobertura actuaría como un distribuidor aleatorio de los datos a través del canal de 22 Mhz de

ancho de banda y la *dispersión* de la señal se llevaría a cabo dentro del codificador DQPSK o DBPSK.

## 2.7 OFDM

Si bien esta técnica no es conocida como una modulación en SS, es empleada en el estándar 802.11a para tasas de transmisión de 6 a 54 Mbps. Orthogonal Frequency Division Multiplexing (OFDM) es una técnica de transmisión multiportadora, la cual divide el espectro disponible en varias portadoras, cada una de ellas modulada por una cadena de datos de menor tasa de transmisión. OFDM es similar a la técnica FDMA[15] en el hecho de que los usuarios pueden acceder a una porción del espectro debido a la división del mismo en múltiples canales. Sin embargo, OFDM utiliza el espectro de una manera mucho más eficiente debido a que permite que el espacio entre canales adyacentes sea muy pequeño. Esto es posible gracias a que todas las portadoras son ortogonales unas respecto a otras, evitándose así, la interferencia entre ellas.

La ortogonalidad de las portadoras significa que cada un de ellas tiene un número entero de ciclos por cada periodo de símbolo. Por ello, el espectro de cada portadora no existe en la frecuencia central de las demás portadoras en el sistema. Esto da como resultado la no interferencia, permitiendo que el espacio entre las portadoras sea lo más cercana posible. Cada portadora en un sistema OFDM tiene un ancho de banda muy reducido (1 KHz), por tanto, la tasa de transmisión de símbolos es muy baja.

OFDM también puede ser utilizado como una modulación en Espectro Disperso (OFDM – SS) donde el ensanchamiento del espectro es acompañado por la inserción de los mismos datos en todas las portadoras, produciendo un factor de dispersión igual al número de portadoras. En el receptor, la energía de todas las portadoras es coherentemente combinada para producir una decisión variable. En la Figura 2.10, se muestra un diagrama de bloques de un sistema transmisor receptor de OFDM – SS.

La generación de la portadora es llevada a cabo eficientemente usando la Transformada Rápida de Fourier Inversa (IFFT) mientras que la demodulación es llevada a cabo por la Transformada Rápida de Fourier (FFT).

[15] Frequency Division Multiple Access

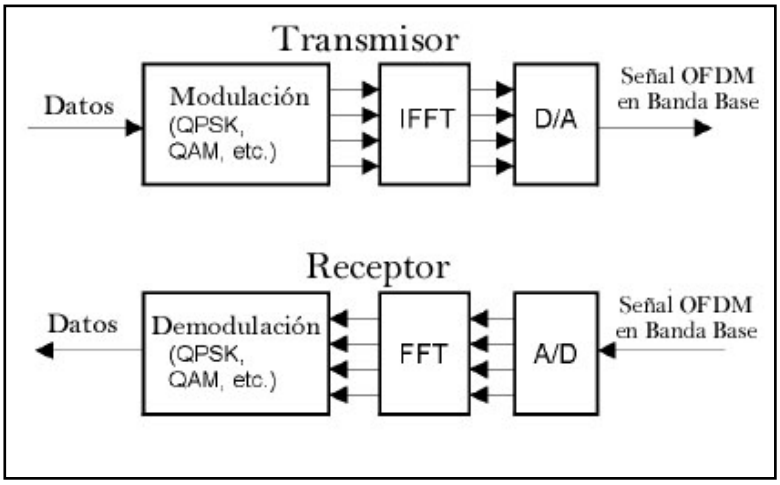



Figura 2.10
*Diagrama de Bloques de un Tx/Rx OFDM*

ODFM–SS tiene muchas de las propiedades de la técnica DSSS. En esencia la principal diferencia entre estos sistemas es que DS utiliza un código de dispersión binario consistentes en 1's y 0's, mientras que OFDM–SS utiliza una forma de onda de dispersión, consistente en una serie de muestras las cuales contienen valores de amplitud no discretos. Sin duda, un modulador de OFDM–SS puede ser construido guardando la forma de onda de dispersión y utilizándola para modular la información de una forma similar a la que es utilizada por los sistemas DSSS. La forma de onda de dispersión es claramente de banda ancha, tal como la secuencia utilizada por DSSS, además, tiene una función de autocorrelación en forma de impulso. Consecuentemente, la señal de OFDM tiene tolerancia a la multitrayectoria y a la interferencia.

### 2.7.1 Generación de una Señal en OFDM

Para generar una señal en OFDM de manera exitosa, la relación entre todas las portadoras debe ser cuidadosamente controlada para mantener la ortogonalidad de las mismas. Por ello, la señal en OFDM es generada seleccionando en primer lugar el espectro requerido, basándose en los datos de entrada y el esquema de modulación utilizado. A cada portadora se le asignan ciertos datos a transmitir. La amplitud y fase que cada portadora requiere, se calculan de acuerdo al esquema de modulación que se haya elegido (típicamente DBPSK, QPSK o QAM). Entonces el espectro requerido es convertido de nueva cuenta a su dominio en el tiempo mediante una Transformada de Fourier Inversa (IFT)[16].

En muchas aplicaciones se utiliza la Transformada Rápida Inversa de Fourier (IFFT). La IFFT lleva a cabo esta transformación de manera eficiente, y proporciona una manera simple de asegurar que las portadoras que se producen son ortogonales. La Transformada Rápida de Fourier (FFT) transforma una señal

[16] Inverse Fourier Transform

periódica en el dominio del tiempo a su equivalente en el dominio de la frecuencia. Esto se realiza encontrando la forma de onda equivalente, generada por la suma de las componentes senoidales ortogonales. La amplitud y fase de las componentes senoidales representan el espectro en frecuencia de la señal que se encuentra en el dominio del tiempo. La IFFT lleva a acabo el proceso inverso, transformando el espectro (amplitud y fase de cada componente) en una señal en el dominio del tiempo. Una IFFT convierte un cierto número de puntos que contienen datos complejos (cuya longitud es un número en potencia de 2) en una señal en el dominio del tiempo que contiene el mismo número de puntos. Cada punto en el dominio de la frecuencia utilizado en la IFFT o FFT se le denomina *bin*. Las portadoras ortogonales requeridas para la señal OFDM pueden ser fácilmente generadas utilizando la amplitud y fase de cada bin, y después aplicando la IFFT.

Debido a que cada *bin* de una IFFT corresponde a una amplitud y fase de un conjunto de señales sinusoidales ortogonales, el proceso inverso garantiza que las portadoras generadas son ortogonales.

## 2.8 Sistemas Infrarrojos

La transmisión/recepción mediante infrarrojos es una de las tres técnicas de modulación definidas en el Estándar IEEE 802.11. Esta técnica difiere de las anteriores debido a que los infrarrojos (IR) utilizan ondas cercanas a la longitud de onda visible como medio de transmisión. Los infrarrojos dependen de la energía que contiene la luz, la cual es reflejada en objetos, o bien, puede propagarse en línea recta. La operación con infrarrojos se reserva a lugares interiores ya que no pueden atravesar objetos sólidos, como es el caso en las técnicas DSSS o FHSSS. En la siguiente figura se muestra un diagrama de bloques básico de un transmisor y receptor IR.

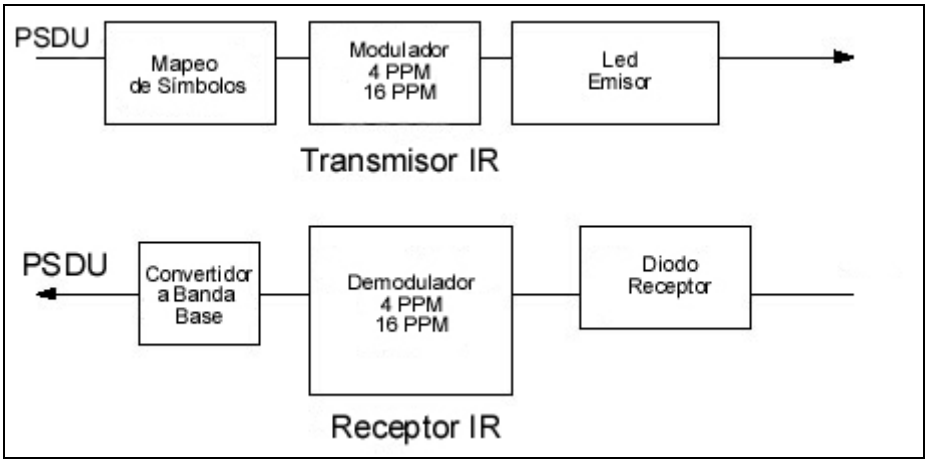



Figura 2.11
*Diagrama de Bloques de un Tx/Rx Infrarrojo*

En IR, las tasas de transmisión son de 1 y 2 Mbps utilizando una técnica las técnicas de modulación 16 PPM[17] y 4 PPM respectivamente. Esta técnica de modulación mantiene la amplitud y el ancho del pulso constantes, variando únicamente la posición del pulso respecto al tiempo. Cada posición en el tiempo representa un símbolo diferente.

[17] Pulse Position Modulation

CAPÍTULO TRES

# El Estándar IEEE 802.11

## 3.1 Introducción

El Estándar IEEE 802.11 define el protocolo y la interconexión de los equipos de datos compatibles a través del *aire* (radio o infrarrojos) en una Red de Área Local (LAN) utilizando el protocolo de Acceso al Medio con Sensor de Portadora/Prevención de Colisión[1] (CSMA/CA), que es un mecanismo definido para compartir el medio.

El Control de Acceso al Medio[2] (MAC) soporta la operación bajo el control de un Punto de Acceso (AP) así como la interoperación de las estaciones independientes. El protocolo CSMA/CA incluye las funciones de autenticación, asociación y reasociación de servicios, un procedimiento opcional de encriptación-*desencriptación*, gestión de potencia para reducir el consumo de energía de estaciones móviles y una función de coordinación puntual para la transferencia de datos.

Las implementaciones utilizando radio en la capa física se especifican en dos modalidades: FHSS y DSSS con tasas de transmisión de 1 y 2 Mbps. La implementación de Infrarrojos en la capa física soporta tasas de transmisión a 1 Mbps con una extensión opcional a 2 Mbps.

A continuación se presenta un breve análisis del Estándar 802.11 cuya versión corresponde a la aprobada en 1999. La primera versión de este estándar fue aceptada en 1997, pero actualmente se emplea como referencia la versión que fue publicada en 1999 pues contiene algunas modificaciones respecto a la primera edición. Algunas de ellas son: se remueve la información base de administración de acuerdo al modelo de referencia OSI así como varios elementos redundantes de administración. Además, se incluye el Anexo D que contiene información base de administración de acuerdo al protocolo SNMP[3]. Hasta el momento este estándar se encuentra sin modificaciones.

[1] Carrier Sense Medium Access/Collision Avoidance
[2] Media Access Control
[3] Simple Name Management Protocol

### 3.1.1 Alcances del Estándar

El alcance de este estándar es el desarrollo de una especificación de la Capa Física (PHY)[4] y de la capa MAC para la conectividad inalámbrica entre equipos portátiles y estaciones móviles dentro de una área local.

### 3.1.2 Objetivo del Estándar

El objetivo del Estándar es el de proporcionar conectividad inalámbrica a máquinas automáticas, equipo o estaciones (STA)[5] que requieren una rápida respuesta, las cuales pueden ser portátiles (estaciones portátiles), o estar instalados en vehículos en movimiento dentro de un área local (estaciones móviles). Una estación portátil es aquélla que cambia de lugar frecuentemente, pero que es utilizada mientras se encuentra en una ubicación determinada. Las estaciones móviles acceden a la LAN mientras se encuentran en movimiento. Los efectos de la propagación marcan la distinción entre las estaciones portátiles y las móviles; las estaciones fijas a menudo se comportan como estaciones móviles debido a dichos efectos de propagación. El estándar también ofrece algunas estructuras regulatorias con la intención de estandarizar los accesos a una o más bandas de frecuencias que tienen la necesidad de comunicación en un área local. Específicamente, este Estándar:

- Describe las funciones y servicios requeridos por los dispositivos compatibles con el Estándar 802.11 para operar dentro de redes de tipo Ad Hoc e Infraestructura, así como los aspectos a considerar de una estación móvil (transición) dentro de esas redes.
- Define los procedimientos de la capa MAC para el soporte de los servicios de entrega de los servicios MSDU[6] asíncronos.
- Define varias técnicas de señalización en la capa física y funciones de interfase que son controladas por la capa MAC definida en este estándar.
- Permite la operación de dispositivos compatibles con este estándar dentro de una WLAN que puede coexistir con múltiples WLAN, pudiendo estar todas ellas superpuestas.
- Describe los requisitos y procedimientos para proporcionar privacidad respecto a la información que los usuarios transmiten sobre un medio inalámbrico, así como la autenticación de los dispositivos que conforman la red.

[4] Physical Layer
[5] STA(estación):Una estación se define como un dispositivo que contiene una interface PHY y MAC conforme al Estándar 802.11 para la transmisión en un medio inalámbrico.
[6] MAC Service Data Unit

## 3.2 El Estándar 802.11 y los Grupos de Trabajo

El Estándar 802.11 define los parámetros de operación de los sistemas que utilizan Espectro Disperso en la capa física; estos parámetros son analizados en diferentes secciones del estándar conocidos como grupos de trabajo. Los siguientes grupos de trabajo contienen descripciones detalladas acerca de las técnicas de modulación empleadas en las WLAN's:

- IEEE 802.11: Operación básica de FHSS y DSSS (Capas Física y MAC) a 1 y 2 Mbps en la banda de 2.4 GHz
- IEEE 802.11a: Operación con OFDM (Capa Física) a 6 – 54 Mbps en la banda de 5 GHz
- IEEE 802.11b: Operación con DSSS (Capa Física) a 5.5 – 11 Mbps en la banda de 2.4 GHz
- IEEE 802.11g: Extensiones al estándar 802.11 b respecto a tasas mayores de transmisión (al menos mayores a 21 Mbps) empleando diversos esquemas de modulación (incluyendo los anteriores e híbridos).

## 3.3 Componentes de la Arquitectura del Estándar 802.11

La arquitectura del Estándar 802.11 consiste en varios componentes que interactúan para proporcionar a las WLAN's la transparencia necesaria hacia capas superiores que soportan estaciones móviles. El Conjunto de Servicios Básicos (BSS) es la configuración básica del Estándar 802.11. Se puede relacionar a este conjunto simplemente con dos o más estaciones que se encuentran dentro de un área donde existe comunicación entre ellas. Cuando una de las estaciones queda fuera del área de cobertura, simplemente deja de pertenecer al BSS.

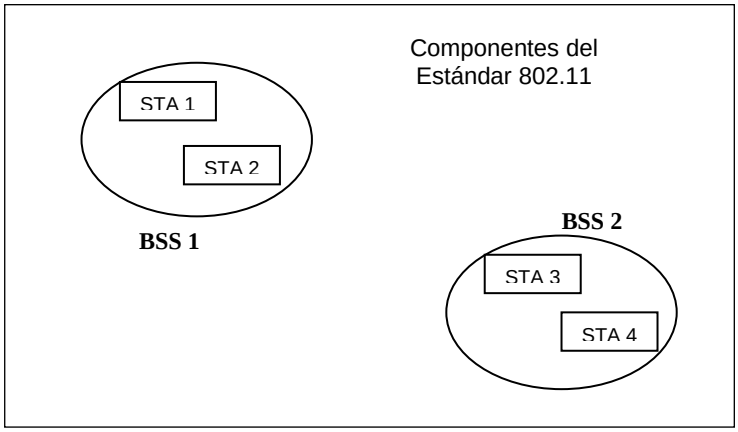



Figura 3.1
*Conjunto de Servicios Básicos (BSS)*

### 3.3.1 Redes Ad Hoc

Los Conjuntos de Servicios Básicos Independientes (IBSS)[7] pertenecen al tipo más común de una WLAN bajo el Estándar 802.11. Para formar esta pequeña red, se requieren al menos dos estaciones que sean capaces de comunicarse directamente. Debido a que este tipo de LAN es frecuentemente formada sin planificación previa y es utilizada mientras se requiera a la red LAN, recibe el nombre de Red Ad Hoc.

La asociación entre una STA y un BSS es dinámica (las estaciones se encienden, se apagan, salen y entran del rango de cobertura). Para ser miembro del BSS, una estación deberá ser *asociada*. Una asociación es un servicio empleado para establecer la ubicación del punto de acceso/estación (AP/STA) y autorizar el acceso de la estación a los Servicios del Sistema de Distribución (DSS)[8]

### 3.3.2 Sistema de Distribución (DS)

Las limitaciones en la capa física PHY determinan la distancia directa que puede ser soportada entre cada una de las estaciones participantes. Para algunas redes ésta distancia puede ser suficiente, mientras que para otras se requiere ampliar el rango de cobertura.

En lugar de existir de manera independiente, un BSS puede formar parte de una red extendida que está constituida por múltiples BSS's. El componente arquitectónico

[7] Independent BSS
[8] Distribution System Services

empleado para interconectar a los BSS's es el Sistema de Distribución (DS)[9]. La distribución es un servicio que utilizando la información de asociación, entrega los MSDU's a la capa MAC dentro de un sistema de distribución. Entonces, el sistema de distribución se encargará de proporcionar la información entre las estaciones que conforman a los diferentes BSS.

La arquitectura de las WLAN's se especifica independientemente de las características físicas de cualquier implementación determinada. El DS hace posible que se puedan emplear dispositivos móviles por medio de servicios lógicos necesarios para manejar ubicaciones de origen y destino, así como la integración de los múltiples BSS's. Un punto de acceso (AP) es una estación (STA) que proporciona el acceso a los servicios del DS, además de actuar como una simple estación. Los datos se mueven entre un BSS y el DS por medio del AP. Como se mencionó anteriormente, los AP's también son estaciones, por lo que son entidades direccionables.

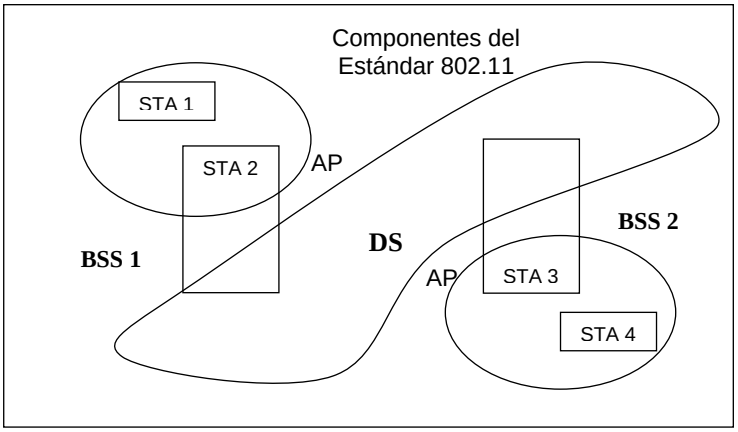



Figura 3.2
*Sistema de Distribución y Puntos de Acceso (AP's)*

### 3.3.3 Redes Tipo Infraestructura

Los DS y los BSS permiten crear una red inalámbrica de tamaño y complejidad arbitraria. El Estándar 802.11 se refiere a este tipo de red como Conjunto Extendido de Servicios (ESS)[10]. Aunque éste es el nombre que se emplea en la norma, a este tipo de redes se les conoce en la literatura hispana como *Redes Tipo Infraestructura.*

[9] Distribution System
[10] Extended Service Set

El concepto clave es que el ESS aparece de la misma forma que un IBSS en la capa LLC[11]. Las estaciones dentro de un ESS pueden comunicarse, y las estaciones móviles pueden cambiar de un BSS a otro (dentro del mismo ESS), todo ello de forma transparente a la capa LLC. Hasta el momento no se ha asumido nada relativo a las ubicaciones físicas de los BSS. Estas ubicaciones pueden ser las siguientes:

1. Los BSS pueden traslaparse parcialmente. Esta configuración se utiliza comúnmente para proporcionar cobertura continua dentro de un volumen físico.
2. Los BSS pueden estar físicamente separados. De manera lógica, no hay límites de distancia entre los BBS's.
3. Los BSS pueden estar físicamente juntos. Esto puede ser posible para proporcionar redundancia.
4. Uno (o más) IBSS o ESS pueden estar presentes físicamente en el mismo espacio como uno (o más) ESS. Esto se debe a las siguientes razones. Una de ellas sucede cuando una Red Ad Hoc opera en el mismo lugar que una Red de tipo Infraestructura; otro caso sucede cuando se traslapan WLAN's debido a que fueron implementadas por diferentes organizaciones.

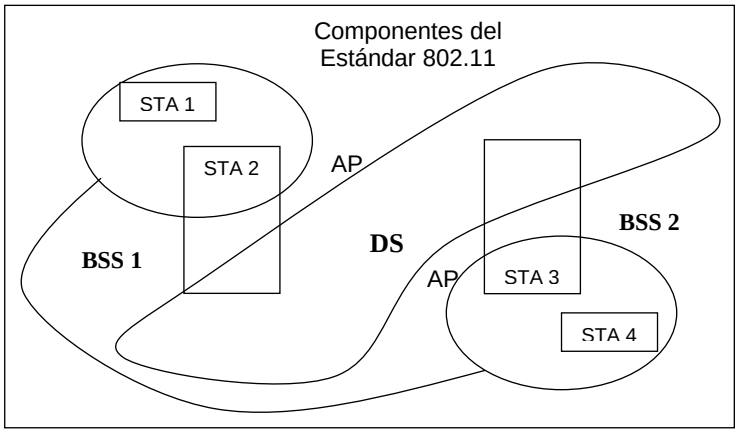



Figura 3.3
*Conjunto Extendido de Servicios*
*(Red Tipo Infraestuctura)*

## Concepto de Área

Las áreas de cobertura bien definidas simplemente no existen para la capa física en un sistema inalámbrico. Las características de propagación son dinámicas e impredecibles. Pequeños cambios en la posición o en la dirección pueden resultar en diferencias considerables en la potencia de la señal. Se pueden observar efectos

[11] Logical Link Control

similares en las STA's ya sean fijas o móviles (por ejemplo, al mover un objeto, éste altera la propagación de la señal aunque la estación se encuentre en una posición fija).

Aunque el término de área es incorrecto para describir la propagación de una señal, dado que ésta se propaga formando un *volumen*, varias aplicaciones utilizan el primer término, ya que es más fácil de representar gráficamente. En el estándar y en la mayoría de la literatura técnica, se emplea el término de *Área*.

### 3.3.4 Integración con Redes LAN

Para integrar una WLAN con una red tradicional (LAN), se utiliza un componente lógico conocido como *portal*. Un portal es un punto lógico en el cual entran MSDU's de una red que no es WLAN a los servicios de distribución (DS) de una WLAN. Es decir, todos los datos generados por una red diferente a las WLAN's entran a la arquitectura de ésta última a través de un *portal*. En la siguiente figura se muestra esta acción. El portal proporciona la integración lógica entre las WLAN's y las redes LAN cableadas existentes. Es posible que un dispositivo sea capaz de ejecutar las funciones de AP y de portal, siempre y cuando sean implementados los servicios de distribución de los componentes de una WLAN. En una WLAN, la arquitectura ESS (que incluyen los AP y los DS's) proporcionan la segmentación del tráfico y la extensión del rango.

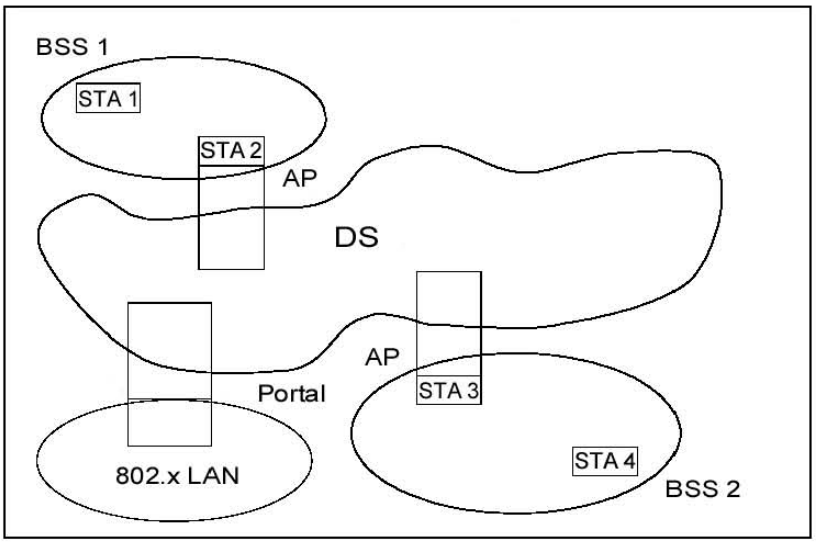



Figura 3.4
*Integración con otras Redes a través de un Portal*

### 3.3.5 Interfaces de Servicios Lógicos

La arquitectura de las WLAN's hace posible que los DS's puedan no ser idénticos a los que existen actualmente en las redes LAN cableadas. Un DS puede ser creado por diferentes tecnologías incluyendo a las actuales LAN. Las WLAN's no restringen el hecho de que los DS's estén basados en la capa de enlace o red (del modelo de referencia OSI), o que los DS's sean de naturaleza centralizada o distribuida, ya que el Estándar 802.11 no especifica explícitamente los detalles de la implementación de los DS's. En vez de ello, el Estándar 802.11 especifica *servicios.*

Los servicios son asociados con diferentes componentes de la arquitectura. Existen dos categorías de servicios en el Estándar 802.11: el servicio de estación y los servicios de distribución del sistema (DSS). Ambas categorías son empleadas por el estándar en la subcapa MAC.

El conjunto de servicios de la arquitectura del Estándar 802.11 es el siguiente:

1. Autenticación
2. Asociación
3. De-autenticación[12]
4. De-asociación[13]
5. Distribución
6. Integración
7. Privacidad
8. Reasociación
9. Entrega de MSDU

Este conjunto de servicios de divide en dos grupos: aquellos que son parte de cada STA y los que son parte de un DS.

#### Servicios de Estación

Los servicios proporcionados por las estaciones se conocen como *servicios de estación.* Los servicios de estación están presentes en cada estación de la red WLAN (incluyendo AP's, así como los AP's incluyen funciones de estación). Los servicios de estación se especifican para ser empleados por las entidades de la subcapa MAC. Los servicios que son proporcionados por las STA son: autenticación, de-autenticación, privacidad y entrega de MSDU's.

[12] Dado que no existe una traducción al castellano de la palabra *deauthentication,* se entiende por dicho término como el proceso mediante el cual una estación no ha sido aceptada como parte del BSS.
[13] Del mismo modo, se entiende por la palabra *deasociation* como el proceso mediante el cual una estación deja de ser parte de un BSS.

Servicios del Sistema de Distribución

Los servicios proporcionados por los DS's se conocen como *servicios del sistema de distribución.* La presencia de varios de los servicios pueden estar o no dentro de un AP físico. Los DSS's son proporcionados por los DS. Éstos son accedidos a través de las STA´s que también proporcionan DSS's. Una STA que proporciona acceso al DSS es un AP.

Los DSS's son los siguientes

a) Asociación
b) De-asociación
c) Distribución
d) Integración
e) Re-asociación

## 3.4 Especificación de la Capa Física (PHY) IEEE 802.11

La capa PHY es la interfase entre la capa MAC y el medio inalámbrico, la cual transmite y recibe los frames de datos sobre un medio inalámbrico compartido. La capa PHY proporciona tres niveles de funcionalidad: en primer lugar, la capa PHY proporciona un intercambio de frames entre la capa MAC y la PHY bajo el control del PLCP[14]. En segundo lugar, la capa PHY emplea la señal de una portadora y la modulación en Espectro Disperso para transmitir frames de datos a través del medio inalámbrico bajo el control del PMD[15]. En tercer lugar, la capa PHY proporciona un sensor de portadora hacia la capa MAC, la cual indica la actividad en el medio. Los términos y las funcionalidades antes mencionadas, se presentan a continuación y son tomados directamente del estándar.

En ésta especificación se describen los servicios de la capa PHY para la subcapa MAC del Estándar 802.11. Se definen diferentes PHY's como parte del Estándar. Cada una de ellas que consisten en dos funciones de protocolo como siguen.

**A.** Una función de convergencia de capa física, la cual adapta las capacidades del sistema dependiente del medio físico (PMD) al servicio de la capa PHY. Esta función es soportada por el procedimiento de convergencia de la capa física (PLCP), el cual define un método de "mapeo" de las unidades de datos de protocolo de la subcapa MAC (MPDU's)[16] dentro de un formato de frame compatible para mandar y recibir datos de los usuarios, así como

[14] Physical Layer Convergence Procedure
[15] Physical Médium Dependent
[16] MAC Protocol Data Units

información de administración entre dos o más STA's que utilicen el sistema PMD asociado.

**B.** Un sistema PMD, cuya función define las características, el método de transmisión y recepción de datos a través del medio inalámbrico (WM)[17] entre dos o más STA's. Cada subcapa PMD puede requerir de la definición de un solo PLCP.

### 3.4.1 Funciones de la Capa PHY

El modelo de referencia para la arquitectura del Estándar 802.11 se muestra en la siguiente figura. La mayoría de las definiciones de la capa PHY contienen tres entidades funcionales: la función PMD, la función de convergencia de la capa física y la función de administración de la capa física.

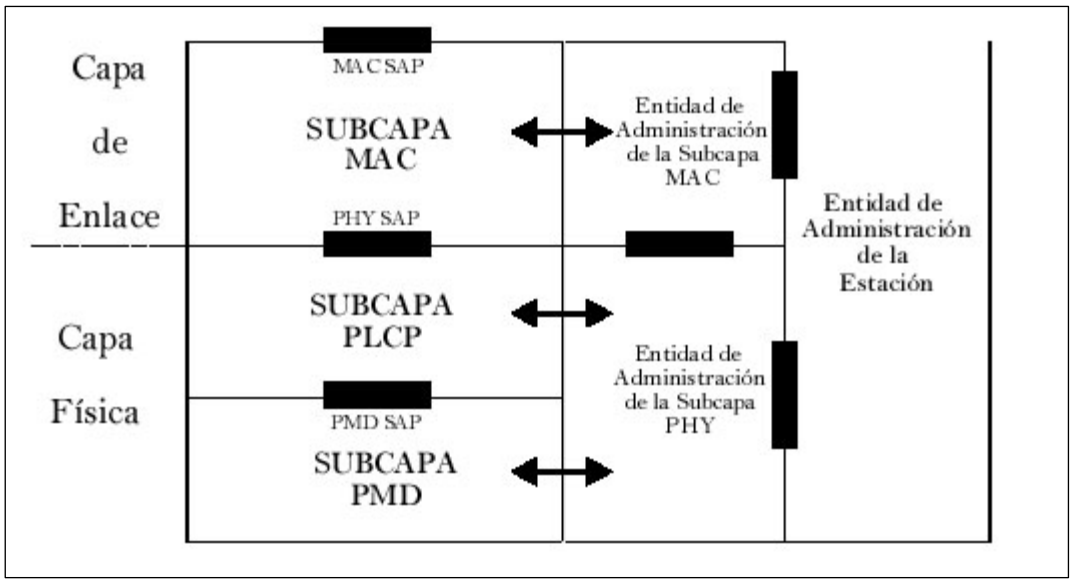



Figura 3.5
*Modelo Básico de Referencia ISO/IEC*

En la función de la capa PHY mostrada, se observa que está separada en dos subcapas: la subcapa PLCP y la subcapa PMD. La función de la subcapa PLCP es la de proporcionar los mecanismos para transferir MPDU's entre dos o más STA's sobre la subcapa PMD.

[17] Wireless Medium

Los detalles de estas funciones se encuentran en la sección 12.3 del Estándar 802.11. En esta sección, se describen los servicios primitivos punto a punto y subcapa-subcapa PHY-SAP[18], (es decir, las interacciones que se realizan entre la capa física PHY y el punto de acceso a los servicios, SAP), las especificaciones de los vectores de transmisión y recepción, y por último, la interacción precisa de este conjunto de especificaciones.

### 3.4.2 Especificación de la Capa Física FHSS

En la subcláusula 14 del Estándar se describen los servicios proporcionados a la subcapa MAC por la capa PHY en los sistemas que emplean Saltos en Frecuencia en Espectro Disperso (FHSS) que opera en la banda de frecuencias de 2.4 GHz. La capa FHSS PHY tiene las mismas funciones que las descritas anteriormente: la función de convergencia de la capa física, el sistema dependiente del medio (PMD) y la función de administración de la capa física. Todas ellas se describen a detalle en la cláusula 14.1.2 del Estándar. A continuación se señalan de forma breve los componentes principales.

Subcapa PLCP FHSS

Esta subcláusula proporciona un procedimiento de convergencia para el mapeo de MPDU's dentro de un formato de frame diseñado para los transmisores y receptores de FHSS.

Formato del Frame PLCP

El formato del frame de las Unidades de Datos del Protocolo PLCP (PPDU)[19] proporcionan la transmisión asíncrona de MPDU's provenientes de la subcapa MAC desde cualquier STA hacia todas las STA's receptoras dentro de los BSS de las WLAN's. EL PPDU mostrado en la figura 3.6 consiste en tres partes: un preámbulo PLCP, un encabezado PLCP y el PSDU[20] (Unidad de Servicio de datos del PLCP).

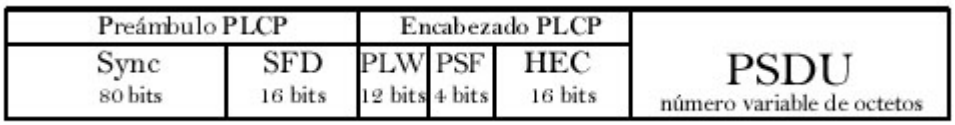



Figura 3.6
*Formato del Frame PLCP FHSS*

[18] Service Access Point
[19] PLCP Protocol Data Unit
[20] PLCP Service Data Unit

El preámbulo proporciona un periodo de tiempo que el receptor emplea para diversas funciones que incluyen la diversidad de las antenas, recuperación del reloj y la delimitación de los campos preámbulo y encabezado. El encabezado PLCP se emplea para especificar la longitud del campo PSDU además de soportar la información de administración del PLCP.

Además, los subcampos especifican lo siguiente:

- ✓ SYNC: Contiene un patrón de unos y ceros con el propósito de detectar una señal que puede ser recibida.
- ✓ SFD[21]: Contiene el siguiente patrón de 16 bits: 0000 1100 1011 1101.
- ✓ PLW[22]: Especifica el número de octetos contenidos en el PSDU.
- ✓ PSF[23]: Indica la tasa de transmisión de los PSDU'S comenzando en 1 Mbps hasta 4 Mbps.
- ✓ HEC[24] : Contiene un campo de 16 bits para la corrección de errores mediante un CRC[25].

## Requisitos Regulatorios

Las implementaciones de las WLAN's que se ajusten a este estándar, están sujetas a la certificación del equipo y requisitos de operación establecidos por órganos reguladores regionales y nacionales. La especificación del PMD establece un mínimo de requisitos técnicos para permitir la interoperabilidad, basados en regulaciones establecidas en Europa, Japón y Estados Unidos al momento en que este estándar fue realizado.

Uno de los principales requisitos técnicos es el del uso de rangos de frecuencia exclusivos. Una implementación que tome en cuenta al PMD, deberá ser capaz de seleccionar una frecuencia de la portadora (Fc) del conjunto de frecuencias disponibles de una cierta región. En la tabla 3.1 se listan algunos países que cuentan con este tipo de regulaciones.

Es preciso tratar con más detalle las regulaciones que son llevadas a cabo en nuestro país. El órgano que regula los asuntos competentes al uso del espectro electromagnético es la Comisión Federal de Telecomunicaciones (COFETEL). Hasta el momento, no existe una definición en el Cuadro Nacional de Atribución de Frecuencias que especifique las restricciones a las que están sujetas la transmisión y

[21] Start Frame Delimiter
[22] PSDU Length Word
[23] PLCP Signaling Field
[24] Header Error Check
[25] Cyclic Redundancy Code

recepción de los sistemas WLAN. Sin embargo, se cuenta con una delimitación en la banda de frecuencias de aplicaciones ICM y de Espectro Disperso.

| Entidad | Límite Inferior | Límite Superior | Rango Especificado |
|---|---|---|---|
| Estados Unidos | 2.402 GHz | 2.480 GHz | 2.400 – 2.4835 GHz |
| Europa[a] | 2.402 GHz | 2.480 GHz | 2.400 – 2.4835 GHz |
| Japón | 2.473 GHz | 2.495 GHz | 2.471 – 2.497 GHz |
| España | 2.447 GHz | 2.473 GHz | 2.445 – 2.475 GHz |
| Francia | 2.448 GHz | 2.482 GHz | 2.4465 – 2.4835 GHz |
| México | - | - | 2.450 – 2.4835 GHz |

[a] Exceptuando a España y Francia

Tabla 3.1
*Rango de Frecuencias Definidas para la Operación de las WLAN's*

A continuación se extrae de dicho documento las especificaciónes para el uso de estas bandas. Se han tomado las bandas superior e inferior en adición a las definiciones de las bandas ICM únicamente con el fin de complementar un marco de referencia para la operación de las WLAN's.

**COMISION FEDERAL**
**DE TELECOMUNICACIONES**

**Cuadro Nacional de Atribución de Frecuencias**
(extracto)

| | |
|---|---|
| Rango de Frecuencia: | **2 360 - 2 450 MHz** |
| Ancho de Banda: | 90 MHz |
| Servicios Atribuidos: | FIJO. Aficionados |
| Cláusulas: | S5.150 / S5.282 |
| Notas MEX[26]: | MEX19 MEX20 MEX21 MEX130 MEX152 MEX153 MEX154 |

**S5.150** Las bandas:

13 553 – 13 567 kHz (frecuencia central 13 560 kHz), 26 957 – 27 283 kHz (frecuencia central 27 120 kHz), 40.66 – 40.70 MHz (frecuencia central 40.68 MHz), 902 – 928 MHz en la Región 2 (frecuencia central 915 MHz), 2 400 – 2 500 MHz (frecuencia central 2 450 MHz), 5 725 – 5 875 MHz (frecuencia central 5 800 MHz) y 24 – 24.25 GHz (frecuencia central 24.125 GHz) están designadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicación que funcionan en estas bandas deben aceptar la

[26] Las notas MEX que no están detalladas en este documento se debe a que carecen de aplicación directa para nuestro estudio.

interferencia perjudicial resultante de estas aplicaciones. Los equipos ICM que funcionen en estas bandas estarán sujetos a las disposiciones del número S15.13.

**MEX130** Las especificaciones para la instalación y operación de sistemas de radiocomunicación que emplean la técnica de espectro disperso en las bandas de 902 - 928 MHz, 2 450 - 2 483.5 MHz y 5 725 - 5 850 MHz, se establecen en la Norma Oficial Mexicana Emergente, NOM-EM-121-SCT1-1994, publicada el 22 de diciembre de 1994 en el Diario Oficial de la Federación. Para evaluar la factibilidad técnica de emplear también la banda 2 400 - 2 450 MHz para espectro disperso, se realizan estudios de convivencia con los sistemas en operación en México.

**MEX152** En la banda 2 300 - 2 450 MHz operan sistemas digitales de multiacceso para proporcionar el servicio de telefonía rural a nivel nacional, asimismo, en esta banda operan sistemas de punto a multipunto para proporcionar el servicio de radiotransmisión de datos a 64 Kb/s para los usuarios dentro de las ciudades más pobladas del país. Ver la nota [MEX153].

**MEX153** En la utilización de la banda 2 300 - 2 450 MHz, se deberá tener en cuenta que en la zona fronteriza de México, colindante con los Estados Unidos de América, no serán posibles las aplicaciones señaladas en la nota [MEX152], ni de radiodifusión sonora digital que proyecta la administración de los Estados Unidos, hasta no contar con procedimientos de coordinación aceptados por ambos países (CAMR-92).

| | |
|---|---|
| Rango de Frecuencia: | **2 450 - 2 483.5 MHz** |
| Ancho de Banda: | 33.5 MHz |
| Servicios Atribuidos: | FIJO. MÓVIL |
| Cláusulas: | S5.150 |
| Notas MEX: | MEX130 |

| | |
|---|---|
| Rango de Frecuencia: | **2 483.5 - 2 500 MHz** |
| Ancho de Banda: | 6.5 MHz |
| Servicios Atribuidos: | FIJO. MÓVIL. MÓVIL POR SATÉLITE (espacio-Tierra) |
| Cláusulas: | S5.150 / S5.402 |
| Notas MEX: | MEX141 |

**S5.402** La utilización de la banda 2 483.5 – 2 500 MHz por el servicio móvil por satélite y el servicio de radiodeterminación por satélite está sujeta a la coordinación a tenor del número S9.11A. Se insta a las administraciones a que tomen todas las medidas necesarias para evitar la interferencia perjudicial al servicio de radioastronomía procedente de las emisiones en la banda 2 483.5 – 2 500 MHz, especialmente la interferencia provocada por la radiación del segundo armónico que caería en la banda 4 990 – 5 000 MHz atribuida al servicio de radioastronomía a escala mundial.

> **MEX141** Las bandas de 1 610 - 1 626.5 MHz y 2 483.5 - 2 500 MHz, también están proyectadas para el servicio móvil por satélite, mediante Satélites de Orbita Baja para transmisiones de voz y datos. Tales satélites deben ser coordinados internacionalmente.

Otra cuestión técnica que el estándar considera es el número de canales utilizados para transmitir o recibir infamación en determinada banda de frecuencias. La entidad PMD utiliza diferentes números de canales disponibles de acuerdo a la región o país. En México no existe una designación de canales para los sistemas WLAN, por lo que la siguiente tabla se muestra como referencia en la designación de dichos canales.

| Entidad | Mínimo de Canales | Número de Frecuencias[a] |
|---|---|---|
| Estados Unidos | 75 | 79 |
| Europa[b] | 20 | 79 |
| Japón | No Aplica | 23 |
| España | 20 | 27 |
| Francia | 20 | 35 |

[a] Se refiere al número de frecuencias elegibles (slots) en las cuales se realizan los saltos.
[b] Exceptuando a Francia y España.

Tabla 3.2
*Rango de Frecuencias Definidas para la Operación de las WLAN's*

Cada uno de estos canales tiene un ancho de banda de 1 MHz por lo que la frecuencia central también varía secuencialmente en 1 MHz comenzando en la frecuencia de 2402 MHz (para el caso de Estados Unidos y la mayor parte de Europa exceptuando a Francia y España) para los canales 2 – 80 y finalizando en 2480 MHz. Para el caso de Japón, los canales disponibles (73 – 95) comienzan en la frecuencia de 2473 MHz y finalizan en 2495 MHz; Francia por su parte dispone de los canales 48 – 82 en el rango de frecuencias de 2448 – 2482 MHz y España los canales 47 – 73 en el rango de 2447 – 2473 MHz.

### Secuencias de Saltos

La secuencia de saltos de una entidad individual PMD se emplea para crear un patrón de saltos pseudo-aleatorios utilizando uniformemente la banda de frecuencias designada. Un conjunto de secuencias de saltos son usados para colocar múltiples entidades PMD en redes similares y en la misma área geográfica, y por otra parte aumentar la eficiencia total y la capacidad de cada red individual.

Un patrón de saltos en frecuencia, *Fx*, consiste en una permutación de todos los canales definidos antes mencionados. Para un cierto número de patrón *X*, la secuencia de saltos se puede escribir como sigue:

$$Fx = \{fx(1), fx(2), \ldots fx(p)\}$$

donde ***fx(i)*** es el número de canal para la i-ésima frecuencia en un cierto número de patrón ***X*** y ***p*** es el número de canales de frecuencia que pueden ser empleados por el patrón de frecuencias. En la sección 14.6.8 del Estándar se describe con detalle la generación de estos patrones de saltos en frecuencia de acuerdo a la región de operación en específico.

### Parámetros de Transmisión y Recepción

En el estándar se especifican diversos parámetros en cuanto a la transmisión y recepción de la señal y a continuación se mencionan los más relevantes:

- ✓ **Modulación**: 2GFSK (Gaussian Frequency Shift Keying) con un periodo de bit nominal (BT) = 0.5. 2GFSK se refiere al hecho de que existen dos desviaciones en frecuencia para codificar los símbolos 0 y 1.

- ✓ **Tasa de transmisión**: Un dispositivo compatible con el Estándar 802.11 debe ser capaz de transmitir y recibir a una tasa de transmisión nominal de 1 Mbps ± 50 partes por millón (ppm).

- ✓ **Nivel de potencia de transmisión**: la potencia de transmisión se especifica a un mínimo de 10 mW de potencia de radiación isotrópica equivalente (EIRP). Si la potencia de transmisión excede de 100 mW, será necesario implementar un control de nivel de potencia.

- ✓ **Sensibilidad del receptor**: se define como el nivel de señal mínimo requerido para asegurar al menos un 3% de error en la recepción de frames. La sensibilidad debe ser menor o igual a -80 dBm.

## Subcapa FHSS PMD, Transmisión a 2.0 Mbps

La transmisión a 2 Mbps contiene muchas de las características de la transmisión a 1 Mbps, y de hecho, todo sistema que sea capaz de transmitir a 2 Mbps, deberá ser capaz de transmitir también a 1 Mbps. Además, los preámbulos del encabezado de la capa física se deberán transmitir a 1 Mbps.

Modulación 4GFSK

El esquema de modulación consiste en cuatro niveles de un cierto factor de desviación de frecuencia. Es decir, una cadena de bits con una tasa de transmisión de 2 Mbps se convertirán en palabras de dos bits (00, 01, 10, 11) que posteriormente serán codificados para resultar en una señal de 4GFSK.

La figura 3.7 una comparación entre los esquemas de modulación 2GFSK y 4GFSK.

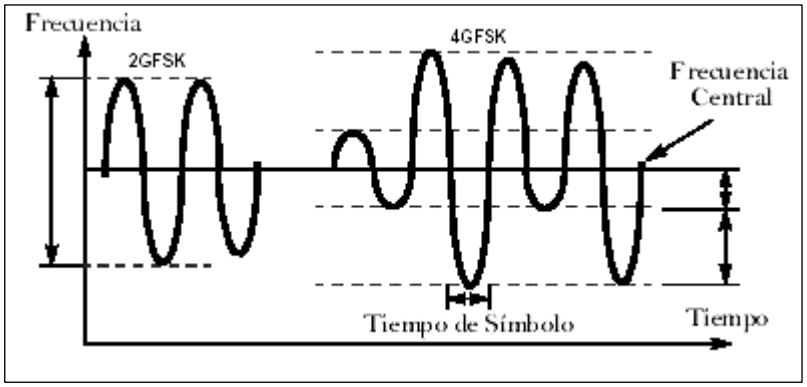



Figura 3.7
*Comparación de las Modulaciones 2GFSK Y 4 GFSK*

### 3.4.3 Especificación de la Capa Física DSSS

En la cláusula 15 del Estándar 802.11 se describe a la capa PHY para los sistemas que operan bajo el esquema DSSS en la banda de 2.4 GHz. El sistema DSSS deberá proporcionar a las WLAN's tasas de transmisión de 1 y 2 Mbps. De acuerdo a las regulaciones de la FCC, el sistema también deberá proporcionar una ganancia de procesamiento de al menos 10 dB; esta ganancia deberá estar asociada al proceso de *chipping* de la señal en banda base a 11 MHz con un código PN de longitud de 11 bits. El sistema DSSS utiliza dos esquemas de modulación para proporcionar las tasas de 1 y 2 Mbps: DBPSK y DQPSK respectivamente.

Las funciones de la capa PHY DSSS son en esencia las mismas que se han descrito con anterioridad. En el apartado 15.1.2 del Estándar se describen con detalle estas funciones.

Subcapa PLCP DSSS

Esta cláusula proporciona un procedimiento de convergencia en el cual los MPDU's son convertidos en PPDU's.

## Formato del Frame PLCP

La siguiente muestra el formato para los PPDU's y se incluyen: el preámbulo DSSS PLCP, el encabezado DSSS PLCP y el MPDU.

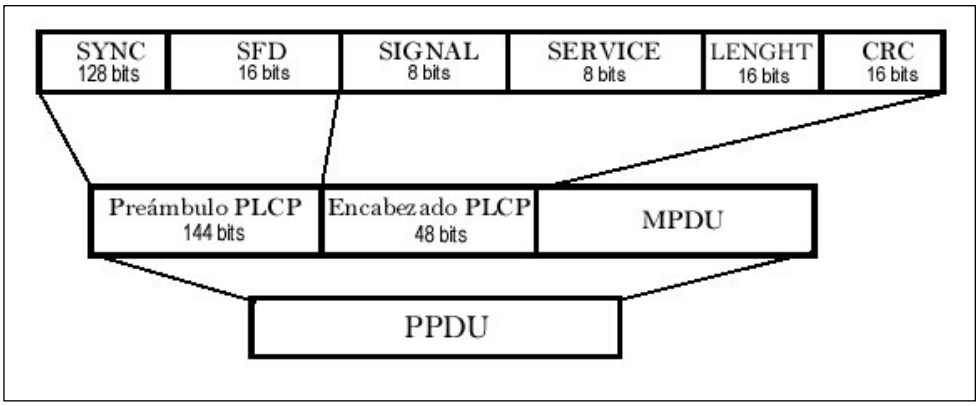



Figura 3.8
*Formato del PPDU para el Esquema DSSS*

Los submódulos contienen lo siguiente:

- ✓ PLCP SYNC: Contiene un patrón de 1's de una longitud de 128 bits.
- ✓ PLCP SFD: Contiene 16 bits y sirve para delimitar el campo actual con el precedente.
- ✓ PLCP Signal: Contiene 8 bits que indica a la capa PHY la modulación que debe ser empleada para la transmisión y recepción de los MPDU's: 1 ó 2 Mbps.
- ✓ PLCP Service: Este submódulo de 8 bits está reservado para futuras aplicaciones. Por el momento indica que los equipos son compatibles con el Estándar 802.11.
- ✓ PLCP Length: Contiene un número entero de 16 bits sin asignar, que indican el número de microsegundos requeridos para transmitir los MPDU's.
- ✓ PLPC CRC: Contiene una secuencia de 16 bits resultantes del código cíclico de redundancia (CRC) el cual protege a los campos Signal, Service y Length.

Requisitos Regulatorios

- ✓ **Frecuencia de Operación**: La capa PHY DSSS debe operar en el rango de frecuencias de 2.4 GHz a 2.4835 GHz en Europa y Estados Unidos, o en el rango de 2.471 a 2.497 GHz en Japón. En México se emplea el rango de 2.450 – 2.4835 GHz, que es la banda asignada para aplicaciones que emplean las técnicas de Espectro Disperso.

- ✓ **Número de Canales de Operación:** De acuerdo a los órganos reguladores de cada país, los canales disponibles se muestran en la siguiente tabla. Los canales que se marcan con una X deberán ser soportados por los dominios regulatorios. El canal 14 está designado para operar exclusivamente en Japón. En México, no existe regulación al respecto, sin embargo (y de acuerdo a algunas implementaciones que se han realizado) se ha establecido el empleo de tres canales que permiten el uso eficiente del ancho de banda designado. Estos canales son el Canal 1 (2.412 GHz), Canal 6 (2.437 GHz) y Canal 11 (2.462 GHz).

| **Países con Canales Definidos** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Número de Canal** | **Frecuencia** | **E. U.** | **Canadá** | **Unión Europea** | **España** | **Francia** | **Japón** |
| 1 | 2412 | X | X | X | - | - | - |
| 2 | 2417 | X | X | X | - | - | - |
| 3 | 2422 | X | X | X | - | - | - |
| 4 | 2427 | X | X | X | - | - | - |
| 5 | 2432 | X | X | X | - | - | - |
| 6 | 2437 | X | X | X | - | - | - |
| 7 | 2442 | X | X | X | - | - | - |
| 8 | 2447 | X | X | X | - | - | - |
| 9 | 2452 | X | X | X | - | - | - |
| 10 | 2457 | X | X | X | X | X | - |
| 11 | 2462 | X | X | X | X | X | - |
| 12 | 2467 | - | - | X | - | X | - |
| 13 | 2472 | - | - | X | - | X | - |
| 14 | 2484 | - | - | - | - | - | X |

Figura 3.3
*Definición de Canales para la operación del DSSS*

En una topología donde existen múltiples células adyacentes y/o sobrepuestas, éstas pueden operar simultáneamente sin interferencia si la distancia entre las frecuencias centrales es de al menos 30 MHz.

## Parámetros de Transmisión y Recepción

La principal diferencia entre los sistemas de Espectro Disperso FHSS y DSSS radica en los esquemas de modulación. En adición a esto, a continuación se detallan los parámetros más relevantes para el esquema DSSS, los cuales también difieren de los presentados para los sistemas FHSS.

- ✓ **Secuencia de Dispersión:** La siguiente secuencia Barker de 11 chips que debe ser empleada como secuencia PN es:

  +1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1

  El chip menos significativo deberá ser el primero en la salida. El primer chip también deberá estar alineado con el inicio del símbolo a transmitir. La duración del símbolo será entonces de 11 bits exactamente.

- ✓ **Modulación y Tasas de Transmisión:** Se especifican dos formatos de modulación y dos tasas de transmisión para la capa PHY DSSS: una tasa *básica* de acceso y otra tasa *aumentada* de acceso. La tasa básica de acceso deberá estar basada en la modulación DBPSK a 1 Mbps. La tasa aumentada de acceso deberá estar basada en la modulación DQPSK a 2 Mbps. En las siguientes tablas se muestra cómo son codificados los símbolos de la cadena de datos entrante.

| Bit de Entrada | Cambio de Fase (+jω) |
|---|---|
| 0 | 0 |
| 1 | π |

Tabla 3.4
*Tabla para la Modulación DSSS a 1.0 Mbps*

| Dibits de Entrada (d0, d1) | Cambio de Fase (+jω) |
|---|---|
| 00 | 0 |
| 01 | π/2 |
| 11 | π |
| 10 | 3π/2 (-π/2) |

Tabla 3.5
*Tabla para la Modulación DSSS a 2.0 Mbps*

- ✓ **Impedancia de las Antenas de Transmisión y Recepción:** La impedancia de los puertos de la antena transmisora y receptora deberá ser de 50 Ω

- ✓ **Niveles de Potencia de Transmisión:** La potencia de salida máxima permitida se especifica de acuerdo a los órganos reguladores de cada país. En la siguiente tabla se muestran estas especificaciones:

| Potencia Máxima de Salida | Ubicación |
|---|---|
| 1000 mW | E. U. |
| 100 mW (EIRP) | Europa |
| 10 mW /MHz | Japón |

Tabla 3.6
*Potencia Máxima de Transmisión en algunos Países*

La potencia mínima de transmisión no deberá ser menor a 1 mW.

- ✓ **Sensibilidad Mínima del Receptor:** La tasa de error en los frames (FER)[27] recibidos debe ser menor que $8x10^{-2}$ para una MPDU de 1024 bytes para un nivel de entrada de -80 dBm medidos en el conector de la antena. Este FER esta especificado para un esquema de modulación de 2 Mbps.

### 3.3.4 Especificación de la Capa Física para Sistemas Infrarrojos

En esta cláusula se especifica la capa física (PHY) para los sistemas infrarrojos (IR). La IR PHY utiliza ondas electromagnéticas cercanas a la luz visible para la señalización en un rango de 850 a 950 nm. Este espectro es similar al utilizado por dispositivos comunes de consumo, tal como los controles remotos infrarrojos y otros dispositivos de comunicación que están avalados por la IrDA (Infrared Data Association).

A diferencia de otros dispositivos infrarrojos, la capa IR PHY no necesita ser dirigida. Esto es, que el receptor y el transmisor no necesitan estar directamente dirigidos uno con respecto del otro y no es necesaria una línea clara de vista. Esto permite la construcción de un verdadero sistema LAN ya que no existen restricciones físicas por lo expuesto anteriormente.

[27] Frame Error Rate

Un par de dispositivos infrarrojos compatibles deberán ser capaces de comunicarse en un rango mayor a 10 m. Este estándar permite la compatibilidad de dispositivos que contengan receptores más sensitivos de manera que el rango sea incrementado a más de 20 m.

La mayoría de los diseños de una red con infrarrojos anticipan que *toda* la energía en el receptor es energía reflejada, aunque la energía puede provenir directamente (en línea de vista) de la fuente o de múltiples reflexiones. Esta modalidad de recepción de energía es llamada Transmisión en *Infrarrojo difuso.*

Éste estándar especifica que el transmisor y el receptor deberán operar en buenas condiciones a pesar de que no exista una línea de vista del transmisor hacia el receptor. Sin embargo, en un ambiente que contenga pocas o ninguna superficie reflejante, el sistema PHY IR puede sufrir de reducción en el rango.

Mientras otros dispositivos de uso común utilizan emisiones infrarrojas en la misma banda óptica, estos dispositivos transmiten usualmente de forma intermitente y no interfieren propiamente con la operación de los equipos compatibles con la capa IR PHY. Si tales dispositivos interfieren debido a la continua transmisión de la señal y ésta es suficientemente fuerte como para obstruir la operación de la red, se puede colocar en otro lugar (otro cuarto, por ejemplo) a la WLAN para aislarla físicamente.

## Subcapa PLCP IR

Proporciona un procedimiento de convergencia por el cual los MPDU's son convertidos en PLCPDU's (unidades de datos del PLCP).

### Formato del Frame

La figura 3.9 muestra el formato del frame que incluyen los campos Preámbulo, Encabezado y el PSDU.

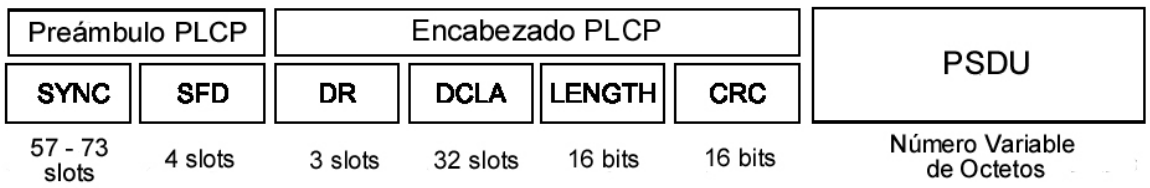



Figura 3.9
*Formato del PPDU para el Esquema IR*

El Preámbulo PLCP se transmitirá empleando los pulsos básicos definidos en la cláusula 16.3.3.2. los campos PLCSDU, Length y CRC deberán ser transmitidos

empleando el esquema de modulación PPM. La modulación PPM mapea los bits en octetos dentro de símbolos: 16 PPM mapea cuatro bits dentro de un símbolo de 16 posiciones, y 4 PPM mapea dos bits dentro de un símbolo de 4 posiciones. La unidad básica de tiempo en el esquema PPM es el slot. Un slot corresponde a una posición cuya duración es de 250 ns. Los campos PLCSDU, Lenght y CRC se transmiten en una de las siguietes tasas de transmisión: 1 y 2 Mbps. El campo Data Rate indica la tasa de transmisión que será empleada para transmitir los campos antes mencionados. Cualquier dispositivo compatible con la capa PHY IR deberá ser capaz de recibir a 1 y 2 Mbps; la transmisión a 2 Mbps es opcional.

Parámetros de Transmisión y Recepción

En esta parte se describen las especificaciones más relevantes para la operación del PMD en cuestiones eléctricas y ópticas requeridas para que sea posible la interoperabilidad de las implementaciones conforme a este estándar. Para obtener información más detallada acerca de éstas especificaciones, se puede consultar la norma en el apartado 16.3.

- ✓ **Modulación y Tasas de Transmisión:** Para la capa física PHY IR se especifican dos tasas de transmisión y dos esquemas de modulación: la tasa *básica de acceso* y la tasa de *aumentada de acceso*. La primera de ellas está basada en el esquema de modulación 16-PPM que entrega una tasa de transmisión de 1 Mbps. La codificación en 16-PPM se especifica en la siguiente tabla. Cada grupo de 4 bits es "mapeado" para formar un símbolo 16-PPM.

| Datos | Símbolo 16 PPM |
|---|---|
| 0000 | 0000000000000001 |
| 0001 | 0000000000000010 |
| 0011 | 0000000000000100 |
| 0010 | 0000000000001000 |
| 0110 | 0000000000010000 |
| 0111 | 0000000000100000 |
| 0101 | 0000000001000000 |
| 0100 | 0000000010000000 |
| 1100 | 0000000100000000 |
| 1101 | 0000001000000000 |
| 1111 | 0000010000000000 |
| 1110 | 0000100000000000 |
| 1010 | 0001000000000000 |
| 1011 | 0010000000000000 |
| 1001 | 0100000000000000 |
| 1000 | 1000000000000000 |

Tabla 3.7
*Codificación 16 – PPM*

La tasa aumentada de acceso se basa en el esquema 4-PPM para entregar una tasa de transmisión de 2 Mbps. En este caso, un grupo de 2 bits es *mapeado* para formar un símbolo 4-PPM.

El orden de transmisión de los símbolos es de derecha a izquierda, como se muestra en la tabla, donde un 1 indica la recepción de energía en el puerto y un 0 indica la ausencia de energía. Esto es, que una cadena de 8 bits será particionada de acuerdo al esquema de modulación (en dos partes para el caso de 16-PPM y en 4 partes para 4-PPM) y después se transmiten los símbolos comenzando por el grupo de bits que está más a la derecha hasta terminar con el último grupo de bits.

| Datos | Símbolo 4 PPM |
|---|---|
| 00 | 0001 |
| 01 | 0010 |
| 11 | 0100 |
| 10 | 1000 |

Tabla 3.8
*Codificación 4 – PPM*

- ✓ **Potencia Óptica de Transmisión:** La potencia de transmisión se muestra en la siguiente tabla.

| **Máscara Patrón de Radiación Emitida** | **Potencia Óptica Pico** |
|---|---|
| Máscara 1 | 2 W ± 20 % |
| Máscara 2 | 0.55 W ± 20 % |

Tabla 3.9
*Potencia de Transmisión Vs. Máscara Patrón*

El proceso de enmascaramiento de la señal a transmitir se describe en el apartado 16.3.3 del estándar, así como otros parámetros significativos. Sin embargo, los detalles de éstas características quedan fuera del alcance de este texto.

## 3.5 El Estándar 802.11a

Esta cláusula especifica a las entidades PHY para un sistema de Multiplexión Ortogonal por División de Frecuencia (OFDM)[28], además de diversos anexos que conforman la base para poder estandarizar la capa OFDM PHY. En este sistema, las radiofrecuencias que son empleadas comprenden los siguientes rangos: 5.15 – 5.25 GHz, 5.25 – 5.35 GHz, y 5.725 – 5.825 GHz que forman parte de de las bandas U-NII (Unlicensed Nacional Information Structure) establecidas por el Código Federal de Regulaciones, en Estados Unidos. En México, únicamente se designa a la banda 5.725 – 5.875 GHz para aplicaciones en la banda ICM.

El sistema OFDM proporciona una estructura WLAN con la capacidad de manejar las siguientes tasas de transmisión: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Es obligatorio que el sistema implementado sea capaz de transmitir y recibir a las tasas de 6, 12 y 24 Mbps. El sistema utiliza 52 subportadoras que son moduladas por los esquemas de modulación BPSK, QPSK, 16-QAM[29] o 64-QAM.

La capa PHY OFDM consiste en dos funciones de protocolo, al igual que las capas PHY mencionadas anteriormente:

a) Una función de convergencia PHY, la cual adapta las capacidades del sistema dependiente del medio físico (PMD) al servicio de la capa PHY. Este servicio es soportado por el procedimiento de convergencia de la capa física (PLCP), que define un método de "mapeo" de las unidades de datos de servicios (PSDU) de la capa PHY dentro de un formato de frame compatible para el envío y recepción de datos de los usuarios, así como información de administración entre dos o más estaciones que utilizan el sistema PMD asociado.
b) Un sistema PMD cuya función define las características y el método de transmisión y recepción de datos a través del medio inalámbrico entre dos o más estaciones, cada una empleando el sistema OFDM.

### 3.4.1 Funciones de la capa PHY OFDM

La arquitectura de la capa OFDM PHY en la banda de 5 GHz está representada en modelo de referencia mostrado en la figura 11 del Estándar 802.11, edición 1999. La capa OFDM PHY contiene tres entidades funcionales: la función PMD, la función de convergencia de la capa PHY y la función de administración de la capa física. Cada una de estas funciones se describe con detalle de la cláusula 17.1.2.1 hasta la 17.1.2.4.

[28] Orthogonal Frequency Division Frequency
[29] Quadrature Amplitude Modulation

El servicio de la capa OFDM PHY hacia la capa MAC se hace a través de servicios primarios descritos en la cláusula 12 del Estándar 802.11, edición 1999.

## Subcapa OFDM PLCP

Esta subcláusula proporciona un procedimiento de convergencia en el cual los PSDU's son convertidos en PPDU's.

### Formato del Frame PLCP OFDM

La figura 3.10 muestra el formato del PPDU que incluye un preámbulo PLCP OFDM, un encabezado OFDM PLCP, el PSDU, bits de cola y de relleno.

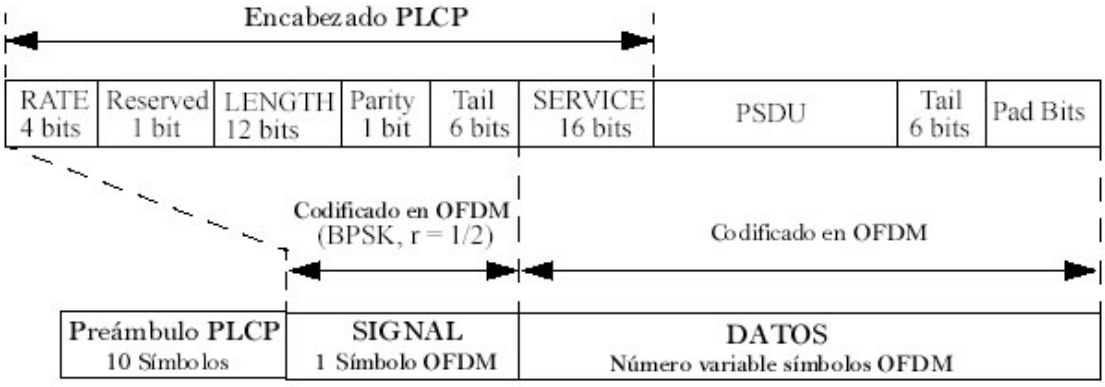



Figura 3.10
*Formato del PLCP para el Esquema OFDM*

Los campos se contienen lo siguiente:

- PREAMBLE: (Sync) Contiene 10 símbolos de corta duración y 2 de larga duración, empleados para la sincronización.
- SIGNAL: Contiene la tasa de transmisión, el tipo de modulación y la longitud del vector de transmisión que está presente en el resto del paquete. Este campo está codificado bajo el esquema BPSK. En el subcampo RATE se especifica la tasa de señalización del paquete mediante el uso de 4 bits. El subcampo LENGHT indica el número de octetos en el PSDU empleando 12 bits para ello.

- DATA: Este campo contiene a los subcampos SERVICE, PSDU, así como los bits de cola y de relleno. El subcampo SERVICE contiene 16 bits, de los cuales, los primeros seis consiste en un conjunto de ceros con el propósito de inicializar al receptor y los bits restantes están reservados hasta el momento. Los bits de cola tienen la función de regresar al estado de "cero" al decodificador convolucional.

## Especificaciones de la Operación de la PMD

Las sub-cláusulas 17.3.8.1 a la 17.3.8.8 del Estándar proporcionan especificaciones generales para las subcapas PMD que emplean los siguientes esquemas de modulacion: BPSK OFDM, QPSK OFDM, 16-QAM OFDM, y 64-QAM OFDM. Estas especificaciones aplican para el transmisor y receptor y en general para la operación de la capa OFDM PHY.

El diagrama de bloques general de un transmisor y receptor de la capa OFDM PHY se muestra en la figura 3.11 y en la tabla 3.10 se muestran especificaciones más concretas de los parámetros de transmisión y recepción de este sistema.

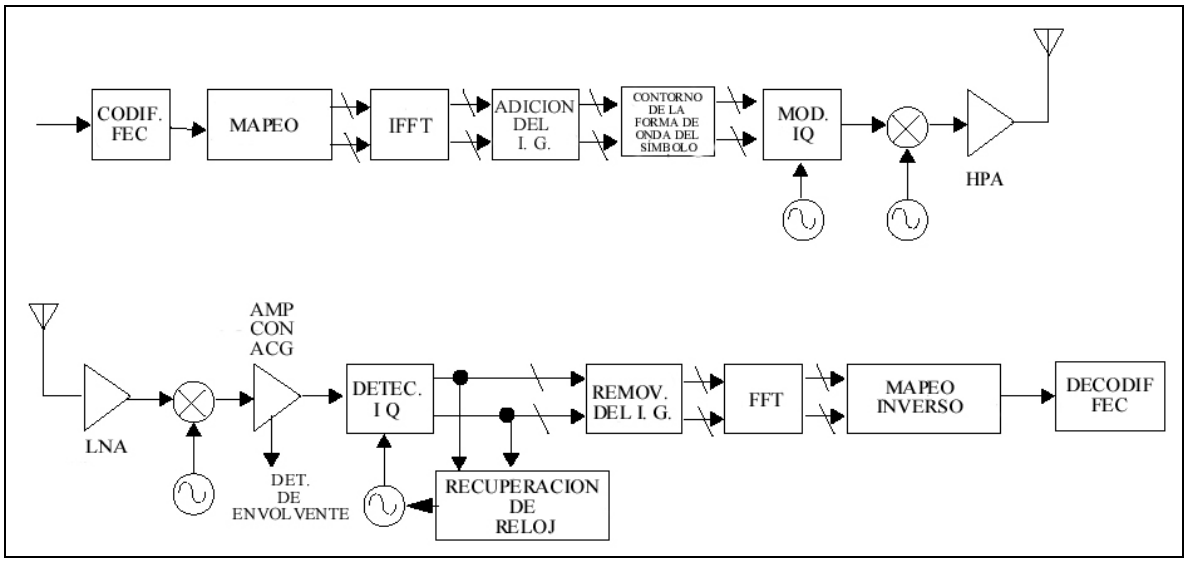



Figura 3.11
*Diagrama de Bloques de un Transmisor / Receptor OFDM*

| | |
|---|---|
| **Información de las Tasas de Transmisión** | 6, 9, 12, 24, 36,<br>48 y 54 Mbps<br>(6, 9 y 12 Mbps son obligatorios) |
| **Modulación** | BPSK OFDM<br>QPSK OFDM<br>16 – QAM OFDM<br>64 – QAM OFDM |
| **Código de Corrección de Errores** | K = 7 (64 estados) códigos convolucionales |
| **Tasa de Codificación** | 1/2, 2/3, 3/4 |
| **Número de Subportadoras** | 52 |
| **Duración del Símbolo OFDM** | 4.0 μs |
| **Intervalo de Guarda** | 0.8 μs[a] ($T_{GI}$) |
| **Ancho de Banda Ocupada** | 16.6 MHz |

[a] Referirse a la subcláusula 17.3.2.4

Tabla 3.10
*Parámetros de Transmisión*
*en el esquema OFDM*

## Requisitos Regulatorios

Las implementaciones de las WLAN de acuerdo con este estándar están sujetas a la certificación del equipo y a los requisitos de operación establecidos por los órganos reguladores nacionales y regionales. La especificación de la PMD establece un mínimo de requisitos técnicos para la interoperabilidad de los sistemas WLAN.

## Rango de las Frecuencias de Operación

La capa OFDM PHY deberá operar en la banda de 5 GHz, de acuerdo al órgano regulador de la región de operación. En el caso de México, la banda de frecuencias disponibles para la operación de la capa OFDM PHY se encuentra en el rango de 5.725 – 5.875 GHz. Dado que no existe un rango de frecuencias específico para la operación de las WLAN's según el estándar, se presentan las bandas de frecuencias que la COFETEL establece para aplicaciones ICM, que son las siguientes:

**COMISION FEDERAL**
**DE TELECOMUNICACIONES**

## Cuadro Nacional de Atribución de Frecuencias

(extracto)

| | |
|---|---|
| Rango de Frecuencia: | 5 650 - 5 830 MHz |
| Ancho de Banda: | 180 MHz |
| Servicios Atribuidos: | RADIOLOCALIZACIÓN.<br>Aficionados |
| Cláusulas: | S5.150 S5.28230 |
| Notas MEX: | MEX19 MEX20 MEX21 MEX130 |

**S5.150** Las bandas:

13 553 – 13 567 kHz (frecuencia central 13 560 kHz), 26 957 – 27 283 kHz (frecuencia central 27 120 kHz), 40.66 – 40.70 MHz (frecuencia central 40.68 MHz), 902 – 928 MHz en la Región 2 (frecuencia central 915 MHz), 2 400 – 2 500 MHz (frecuencia central 2 450 MHz), 5 725 – 5 875 MHz (frecuencia central 5 800 MHz) y 24 – 24.25 GHz (frecuencia central 24.125 GHz) están designadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicación que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones. Los equipos ICM que funcionen en estas bandas estarán sujetos a las disposiciones del número S15.13.

MEX20 Las especificaciones técnicas que deben cumplir los equipos y accesorios utilizados por las estaciones de aficionados, así como las disposiciones respecto a la instalación y operación del equipo y la ubicación de las instalaciones, se establecen en la Norma Oficial Emergente, NOM-EM-086-SCT1-1994, publicada el 15 de diciembre de 1994 en el Diario Oficial de la Federación. Bandas comprendidas: 1 800 - 1 850 kHz, 7 000 - 7 300 kHz, 14 000 - 14 350 kHz, 18 068 - 18 168 kHz, 21 000 - 21 450 kHz, 24 890 - 24 990 kHz, 28 000 - 29 700 kHz, 50 - 54 MHz, 144 - 148 MHz, 220 - 225 MHz, 24 - 24.05 GHz, 47 - 47.2 GHz, 75.5 - 76 GHz, 142 - 144 GHz, 248 - 250 GHz, 1 850 - 2 000 kHz, 3 500 - 4 000 kHz, 10 100 - 10 150 kHz, 430 - 440 MHz, 1 240 - 1 300 MHz, 2 300 - 2 450 MHz, 3 300 - 3 500 MHz, 5 650 - 5 925 MHz, 10 - 10.5 GHz, 24.05 - 24.25 GHz, 76 - 81 GHz, 144 - 149 GHz, 241 - 248 GHz.

MEX130 Las especificaciones para la instalación y operación de sistemas de radiocomunicación que emplean la técnica de espectro disperso en las bandas de 902 - 928 MHz, 2 450 - 2 483.5 MHz y 5 725 - 5 850 MHz, se establecen en la Norma Oficial Mexicana Emergente, NOM-EM-121-SCT1-1994, publicada el 22 de diciembre

[30] Las cláusulas y las notas MEX que no son mencionadas en este documento, pueden ser consultadas en el Cuadro Nacional de Atribución de Frecuencias.

de 1994 en el Diario Oficial de la Federación. Para evaluar la factibilidad técnica de emplear también la banda 2 400 - 2 450 MHz para espectro disperso, se realizan estudios de convivencia con los sistemas en operación en México.

| | |
|---|---|
| Rango de Frecuencia: | 5 830 - 5 850 MHz |
| Ancho de Banda: | 20 MHz |
| Servicios Atribuidos: | RADIOLOCALIZACIÓN. Aficionados. Aficionados por satélite (espacio - Tierra) |
| Cláusula: | S5.150 |
| Notas MEX: | MEX19 MEX20 MEX21 MEX130 |

| | |
|---|---|
| Rango de Frecuencia: | 5 850 - 5 925 MHz |
| Ancho de Banda: | 75 MHz |
| Servicios Atribuidos: | FIJO. FIJO POR SATÉLITE (Tierra – espacio). Aficionados. |
| Cláusula: | S5.150 |
| Notas MEX: | MEX19 MEX20 MEX21 MEX170 |

MEX170 La banda de 5 850 - 8 500 MHz se utiliza extensamente por el servicio fijo multicanal para sistemas de microondas punto a punto.

## Parámetros Dependientes de la Modulación

Éstos parámetros están definidos en la siguiente tabla:

| **Tasa de Transmisión (Mbps)** | **Modulación** | **Tasa de Codificación (R)** | **Bits Codificados por Subportadora ($N_{BPSC}$)** | **Bits Codificados por cada Símbolo OFDM ($N_{CBPS}$)** | **Bits de Datos por cada Símbolo OFDM ($N_{DBPS}$)** |
|---|---|---|---|---|---|
| 6 | BPSK | 1/2 | 1 | 48 | 24 |
| 9 | BPSK | 3/4 | 1 | 48 | 36 |
| 12 | QPSK | 1/2 | 2 | 96 | 48 |
| 18 | QPSK | 3/4 | 2 | 96 | 72 |
| 24 | 16 – QAM | 1/2 | 4 | 192 | 96 |
| 36 | 16 – QAM | 3/4 | 4 | 192 | 144 |
| 48 | 64 – QAM | 2/3 | 6 | 288 | 192 |
| 54 | 64 – QAM | 3/4 | 6 | 288 | 216 |

Tabla 3.11
*Parámetros Dependendientes de la modulación*

## 3.6 El Estándar 802.11b

Esta cláusula especifica la extensión de la capa PHY en altas tasas de transmisión para un sistema DSSS (cláusula 15 del Estándar IEEE 802.11 edición 1999) en la banda de 2.4 GHz diseñada para aplicaciones ICM.

Esta extensión del sistema DSSS incrementa las capacidades de las tasas de transmisión descritas en la cláusula 15, para proporcionar tasas de transmisión de 5.5 y 11 Mbps adicionales a las tasas que maneja dicho estándar que son de 1 y 2 Mbps. La tasa del *chipping* es de 11 MHz al igual que sistema DSSS del Estándar 802.11, por lo que ocupa el mismo ancho de banda. Para proporcional tasas más altas de transmisión, se emplea el esquema de modulación CCK de 8 bits de longitud.

La capa PHY emplea para altas tasas de transmisión el mismo preámbulo en el PLCP que la capa DSSS PHY, por lo que ambos sistemas pueden coexistir en el mismo BSS utilizando un mecanismo de cambio (switching) que se proporciona en este estándar.

Un modo opcional de proporcionar tasas de transmisión de 2, 5.5 y 11 Mbps se logra a través del uso del método PBCC, el cual utiliza un preámbulo PLCP más corto, incrementando de esta manera la eficiencia del sistema en forma significativa.

En general, esta extensión del estándar especifica las entidades de la capa PHY para las extensiones de un sistema de alta velocidad DSSS. La capa PHY de alta velocidad consiste en las siguientes dos funciones de protocolo:

**A.** Una función de convergencia de la capa PHY, la cual adapta las capacidades del sistema PMD a los servicios de la capa PHY. Esta función es soportada por el procedimiento de convergencia de la capa PHY (PLCP), que define un método de "mapeo" de las unidades de datos de protocolo de la subcapa MAC (MPDU) dentro de un formato de frame compatible para la transmisión y recepción de los datos de los usuarios, así como la información de administración entre dos o más STA's que emplean el mismo sistema PMD asociado.

**B.** Un sistema PMD, cuya función define las características y los métodos de transmisión y recepción de los datos a través del medio inalámbrico, entre dos o más estaciones, cada una de ellas empleando un sistema PHY de alta velocidad.

### 3.6.1 Funciones de la Capa PHY HR

La arquitectura de la capa PHY HR[31] en la banda de 2.4 GHz está representada en el modelo básico de referencia ISO/IEC mostrado en la figura 3.5. La capa PHY HR contiene tres entidades fundamentales: la función PMD, la función de convergencia de la capa PHY y la función de administración de capa. Cada una de estas funciones se describen con detalle en las cláusulas 18.1.2.1, 18.1.2.2, y 18.1.2.3. Los servicios de las capas PHY HR deberán ser proporcionados a la capa MAC a través de los servicios primarios descritos en la cláusula 12 del Estándar IEEE 802.11, edición 1999.

Subcapa HR PLCP

Esta subcláusula proporciona un procedimiento de convergencia para las especificaciones de las tasas a 2, 5.5 y 11 Mbps, en las cuales los PSDU's son convertidos en PPDU's. Se definen dos preámbulos diferentes: el encabezado largo que debe ser soportado de manera obligatoria y que puede interoperar con las especificaciones del Estándar 802.11 respecto a las tasas de transmisión de 1 y 2 Mbps, y por otra parte, un preámbulo y encabezado cortos opcionales.

El preámbulo corto opcional y el encabezado están dirigidos hacia aplicaciones donde se desea la máxima tasa de transmisión efectiva, además de que se espera que sean empleados en equipos que sean capaces de manejar los modos opcionales.

Formato Largo PPDU PLCP

La figura 3.12 muestra el formato para el PPDU interoperable, incluyendo el preámbulo HR PLCP, el encabezado HR PLCP y el PSDU

El formato para el PPDU, incluyendo el preámbulo largo HR PLCP, el encabezado largo HR PLCP y el PSDU, no difieren de los especificados en el Estándar 802.11, edición 1999 para 1 y 2 Mbps, a excepción de las siguientes consideraciones:

a) La codificación de la señalización en el campo SIGNAL
b) El uso de un bit en el campo SERVICE para resolver una ambigüedad en la longitud de los octetos del PSDU, cuando la longitud es expresada en microsegundos
c) El uso de un bit en el campo SERVICE para indicar que el modo opcional PBCC está siendo empleado

[31] High Rate

d) El uso de un bit en el campo SERVICE para indicar que la frecuencia de transición y los bits de reloj se encuentran bloqueados.

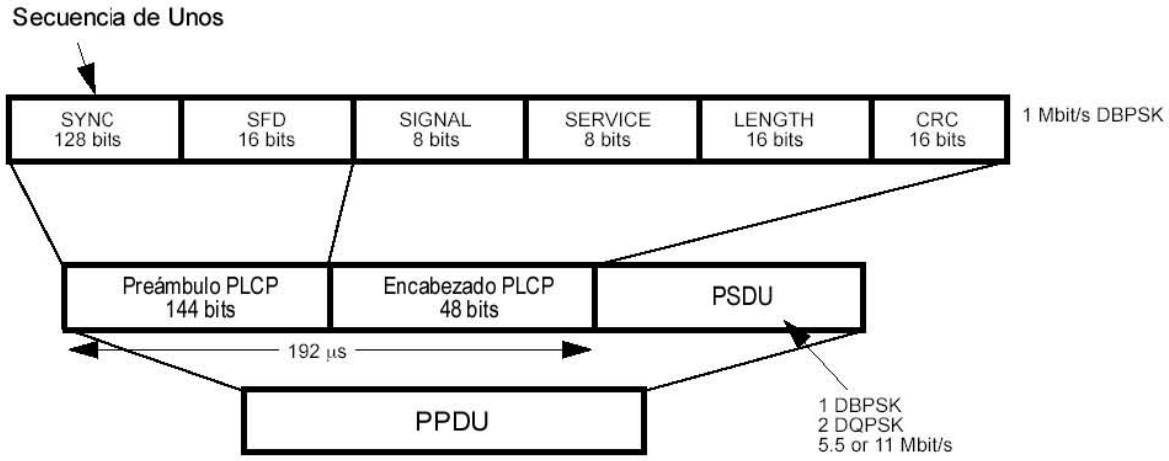



Figura 3.12
*Formato Largo PLPC PPDU*
*para la capa PHY HR*

Los subcampos contienen la siguiente información

- ✓ SYNC: Contiene 128 bits que sirven para lograr la sincronización con el receptor
- ✓ SFD: (Start Frame Delimiter). Indica el comienzo de los parámetros PHY dentro del preámbulo PLCP, y contiene 16 bits.
- ✓ SIGNAL: Contiene 8 bits que le indican a la capa PHY la tasa de señalización que será empleado para la transmisión y recepción de los PSDU.
- ✓ SERVICE: Contiene 8 bits, de los cuales el bit 2 indica si los bits de reloj se encuentran bloqueados, el bit 3 indica el tipo de modulación (PBCC o CCK) y los demás bits se encuentran reservados.
- ✓ LENGHT: Deberá contener 16 bits sin asignar, ya que estos bits serán determinados de acuerdo a los parámetros del vector de transmisión. Indica el número de microsegundos requeridos para transmitir el PSDU.
- ✓ CRC: Contiene 16 bits resultado de un CRC.

Como puede observarse en la figura, el encabezado y el preámbulo deberán transmitirse a 1 Mbps empleando el esquema DBPSK.

## Formato Corto PPDU PLCP

El preámbulo PLCP y el encabezado se define de manera opcional, con el propósito de minimizar el tamaño del encabezado y por ende, maximizar la tasa de transmisión efectiva del sistema. El formato del PPDU se muestra en la figura 3.13.

Un transmisor que emplea el PLCP corto, es capaz de interoperar con otro receptor que también sea capaz de recibir este PLCP corto. Para interoperar con un receptor que no es capaz de recibir los PLCP's cortos, el transmisor deberá emplear el preámbulo y encabezado PLCP largo. El preámbulo PLCP corto emplea el código de dispersión Barker a 1 Mbps bajo el esquema DBPSK. El encabezado PLCP corto emplea el código de dispersión Barker con modulación DQPSK, y el PSDU es transmitido a 2, 5.5 u 11 Mbps.

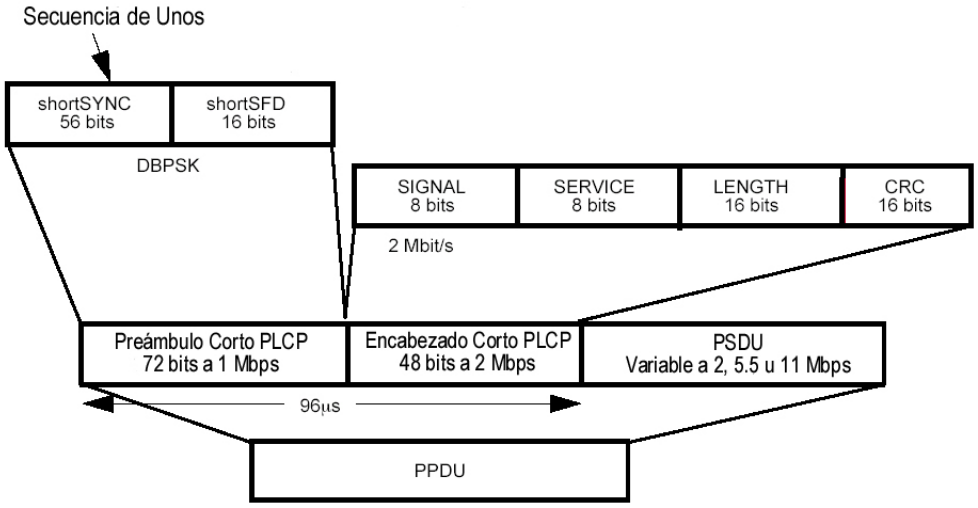



Figura 3.13
*Formato Corto PLPC PPDU*
*para la capa PHY HR*

Los subcampos contienen la siguiente información:

- ✓ shortSYNC: Contiene 56 bits que proporciona al receptor la información necesaria para la sincronización.
- ✓ shortSFD: Consiste en un patrón de 16 bits (0000 0101 1100 1111) que indica el comienzo de los parámetros PHY. Un receptor que no esté configurado para emplear los encabezados cortos, no detectará el SFD.
- ✓ shortSIGNAL: Contiene 8 bits que indican a la capa PHY la tasa de transmisión que deberá ser empleada para la transmisión (y recepción) del PSDU.

Los subcampos SERVICE, LENGTH, y CRC deberán ser los mismos que los descritos en el encabezado PLCP largo.

### Frecuencias de Operación

La capa PHY HR deberá operar en el rango de frecuencias 2.4 – 2.4835 GHz, como lo indican los órganos reguladores en Estados Unidos y Europa. Dado que el sistema de alta velocidad opera en la misma banda de frecuencias que los sistemas con tasa de transmisión básica (1 y 2 Mbps), se tienen las mismas consideraciones regulatorias en México, como se describió en el análisis de dichas tasas de transmisión.

### Número de Canales

A pesar de que si existe regulación en México respecto a las bandas de frecuencia designadas para la transmisión en espectro disperso, no se especifican las frecuencias centrales de cada canal, por lo que a manera de ejemplo, se muestra la tabla 3.11 donde se especifican los canales que se han asignado en diferentes países que cuentan con regulación al respecto.

En una topología que contenga múltiples células, se pueden emplear diferentes canales sin que exista interferencia para células que sean adyacentes o que se traslapen, sólo si la distancia entre las frecuencias centrales es de al menos de 25 MHz.

### Modulación y Tasas de Transmisión

Para la capa PHY HR se especifican cuatro formatos de modulación. La tasa *básica de acceso* deberá estar basada en la modulación DBPSK a 1 Mbps. La tasa *aumentada de acceso* deberá estar basada en el esquema DQPSK a 2 Mbps. La extensión de la especificación para la secuencia directa define dos tasas de transición adicionales. Los accesos en HR deberán estar basados en el esquema de modulación CCK para 5.5 y 11 Mbps. Un modo opcional es también proporcionado para mejorar el rendimiento del sistema empleando la técnica PBCC.

| | | Dominios Regulatorios | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ID del Canal | Freq. (Mhz) | FCC | IC | ETSI | España | Francia | Japón | Japón |
| 1 | 2412 | X | X | X | — | — | — | X |
| 2 | 2417 | X | X | X | — | — | — | X |
| 3 | 2422 | X | X | X | — | — | — | X |
| 4 | 2427 | X | X | X | — | — | — | X |
| 5 | 2432 | X | X | X | — | — | — | X |
| 6 | 2437 | X | X | X | — | — | — | X |
| 7 | 2442 | X | X | X | — | — | — | X |
| 8 | 2447 | X | X | X | — | — | — | X |
| 9 | 2452 | X | X | X | — | — | — | X |
| 10 | 2457 | X | X | X | X | X | — | X |
| 11 | 2462 | X | X | X | X | X | — | X |
| 12 | 2467 | — | — | X | — | X | — | X |
| 13 | 2472 | — | — | X | — | X | — | X |
| 14 | 2484 | — | — | — | — | — | X | — |

Tabla 3.12
*Plan de Frecuencias*
*para Canales HR PHY*

## Secuencias de Dispersión y Modulación

### Para 1 y 2 Mbps

La siguiente secuencia Barrer de 11 chips de longitud deberá ser empleada como la secuencia de código PN para las tasas de transmisión de 1 y 2 Mbps

+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1

El bit menos significativo deberá salir en primer lugar. El primer chip transmitido deberá estar alineado con el comienzo del primer símbolo. La duración de cada símbolo deberá tener una longitud exacta de 11 chips. La codificación en DBPSK para el acceso básico se especifica en la tabla 106 del estándar. La codificación en

DQPSK se especifica en la tabla 107 del estándar. (En ésas tablas, +jω deberá ser definido en sentido de la rotación de las manecillas del reloj).

**Esquema CCK a 5.5 y 11 Mbps**

Para los modos de modulación CCK, la longitud del código de dispersión es de 8 bits, basándose en los códigos complementarios. La tasa de *chiping* es de 11 Mchip/s. La duración del símbolo deberá ser de 8 bits complejos de longitud. La siguiente fórmula deberá ser usada para determinar las palabras de código CCK que serán utilizadas para lograr las tasas de transmisión de 5.5 y 11 Mbps.

$$C = \left\{ \begin{matrix} e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, \\ e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \end{matrix} \right\}$$

Donde C es la palabra de código C = {c0 to c7}.

Los términos φ1, φ2, φ3, y φ4 están definidos en las cláusulas 18.4.6.5.2 para la tasa de 5.5 Mbps y en la cláusula 18.4.6.5.3 para 11 Mbit/s. La fórmula crea 8 chips complejos (c0 a c7), donde c0 es transmitido en primer lugar. La generación de los chips complejos se describió con detalle en el capítulo anterior.

Modulación Opcional en PBCC

Este esquema de codificación opcional emplea una codificación binaria convolucional, que consiste en utilizar un código binario convolucional (BCC)[32] de 64 estados y una secuencia de cobertura. La salida de la BCC es codificada en los canales Q e I, como se describió en el capítulo anterior. El código de cobertura es aplicado a los datos ya codificados antes de ser transmitidos a través del canal.

La tasa de transmisión de 5.5 Mbps emplea el esquema de modulación BPSK y la tasa de 11 Mbps emplea QPSK. En el modo QPSK, cada par de bits de salida del código convolucional son empleados para producir un símbolo; en el modo BPSK, cada par de bits del BCC se toman en serie y se emplean para producir dos símbolos BPSK. Esto da como resultado que se obtenga un bit por símbolo en el modo QPSK y medio bit por símbolo en el modo BPSK.

[32] Binary Convolutional Code

Parámetros de Transmisión y Recepción

- ✓ **Impedancia del puerto de la antena**: Deberá ser de 50 Ω si el puerto es expuesto.

- ✓ **Niveles de Potencia de Transmisión**: La potencia de salida máxima permisible debe estar sujeta a las especificaciones de cada país o región. Al respecto, aún no existe en México regulación en esa materia; sin embargo, con fines de ejemplo, se menciona que en Estados Unidos la potencia máxima de transmisión es de 1 W y 100 mW (EIRP) para Europa.

- ✓ **Nivel de Control de Potencia**: El control de potencia deberá proporcionarse para potencias de transmisión mayores a 100 mW. También se deben proporcionar un máximo de cuatro niveles de potencia distintos. Como mínimo, el sistema que transmite a una potencia mayor a 100 mW también deberá ser capaz de hacer el cambio a una potencia de 100 mW o menos. En las subcláusulas 18.4.8.1 a la 18.4.8.4 se describe las funciones del receptor y los parámetros asociados con la subcapa PMD.

- ✓ **Sensitividad Mínima del Receptor**: La tasa de error del frame (FER)[33] deberá ser menor que $8x10^{-2}$ para un PSDU de longitud igual a 1024 octetos con un nivel de entrada de -76 dBm medidos en el conector de la antena. Este FER está especificado para la modulación CCK a 11 Mbps.

- ✓ **Nivel Máximo de Recepción**: El receptor deberá proporcionar un FER de $8x10^{-2}$ para un PSDU de longitud de 1024 octetos para un nivel de entrada máximo de -10 dBm medido en la antena. De la misma manera, este FER está especificado para la modulación CCK a 11 Mbps.

## 3.7 El Estándar IEEE 802.11 g

Esta cláusula especifica otra extensión más a las tasas de transmisión en la capa PHY para el sistema DSSS, descrito en la cláusula 15 (Estándar 802.11, edición 1999) y en la extensión de la cláusula 18 (Estándar 802.11b). De aquí en adelante la capa PHY definida en este estándar será llamada ERP, cuyas siglas corresponden a Extended Rate PHY. Esta capa PHY opera en la banda de frecuencias para aplicaciones ICM de 2.4 GHz.

[33] Frame Error Rate

La ERP trabaja con las tasas de transmisión de 1 y 2 Mbps, como se describe en la cláusula 15 (Estándar 802.11) y emplea el esquema DSSS; también es capaz de manejar las tasas de 1, 2, 5.5 y 11 Mbps, como se describe en la cláusula 18 (Estándar 802.11b) que también emplea los esquemas DSSS, CCK y PBCC. La ERP se basa en la cláusula 17 (Estándar 802.11a) para proporcionar adicionalmente las siguientes tasas de transmisión: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. De estas tasas, son obligatorias las capacidades de los sistemas para transmitir y recibir en las siguientes tasas: 1, 2, 5.5, 11, 6, 12, y 24 Mbps. También se definen dos tipos de modulación opcionales con tasas de transmisión de 22 y 33 Mbps empleando el esquema PBCC, y que se denomina como ERP – PBCC. También se incorpora una modulación opcional conocida como DSSS – OFDM con tasas de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

### 3.7.1 Modos de Operación

La ERP tiene la capacidad de decodificar todos los PLCP's descritos en las cláusulas 15 y 18, así como los PLCP's de los sistemas ERP – OFDM. En adición, es obligatorio todos los equipos compatibles con la ERP deben ser capaces de enviar y recibir los preámbulos cortos que son opcionales para la cláusula 18.

Un BSS que opera en la ERP debe ser capaz de operar en cualquier combinación de los modos ERP disponibles (cláusula 19 PHY's) y los modos distintos a la ERP (cláusula 15 o cláusula 18). Por ejemplo, un BSS podría operar en un esquema ERP – OFDM únicamente, o en un modo mixto con los esquemas ERP – OFDM y ERP – DSSS/CCK, o bien, otro modo mixto con los esquemas ERP – DSSS/CCK y FHSS.

Los cambios que requiere el estándar base para implementar la ERP se resumen como sigue:

**A. ERP – DSSS/CCK**

1. La PHY emplea las capacidades del la cláusula con las siguientes excepciones:
    a. Es obligatorio el soporte del formato corto de encabezado PLCP de la cláusula 18.2.2.2
    b. El nivel máximo de la señal de entrada (ver 18.4.8.2) es de 20 dBm.
    c. Es obligatorio el bloqueo de la frecuencia central de transmisión y de la frecuencia de reloj del mismo oscilador de referencia.

**B. ERP – OFDM**

1. La capa PHY emplea las capacidades de la cláusula 17 con las siguientes excepciones:

a. El plan de frecuencias es el especificado en la cláusula 18.4.6.1 y 18.4.6.2 en lugar de la cláusula 17.3.8.3.
b. El nivel máximo de la señal de entrada (ver 17.3.10.4) es de -20 dBm.
c. El tiempo del slot es de 20 μs de (acuerdo a la cláusula 18.3.3) a excepción de que un tiempo de slot de 9 μs es empleado cuando un BSS consiste en una sola STA ERP.

**C. ERP – PBCC (opcional)**

1. Este esquema de modulación de una sola portadora emplea un código binario convolucional de 256 estados. Este modo es una extensión de la modulación PBCC descrito en la cláusula 18. Los modos con tasas de transmisión de 22 y 33 Mbps se definen en la cláusula 19.6.

**D. DSSS – OFDM (opcional)**

1. Ésta es una modulación híbrida que combina un preámbulo y encabezado DSSS con una transmisión del PPDU modulado con OFDM. Los modos DSSS – OFDM operan con tasas de transmisión de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps y se definen en la cláusula 19.7
2. Si se emplea el modo opcional DSSS – OFDM, las tasas de transmisión en dicho modo de operación serán las mismas que las tasas empleadas por el modo ERP – OFDM.

### 3.7.2 Funciones de la ERP

La arquitectura de la ERP está representada en el modelo de referencia ISO/IEC, mostrado en la figura 3.5. La ERP contiene tres entidades funcionales: la función PMD, la función de convergencia de la capa PHY y la función de administración de capa. Los servicios de la ERP para la capa MAC son proporcionados a través de los servicios primarios descritos en la cláusula 12. La interoperabilidad se encuentra a cargo del mecanismo de acceso al medio especificado en la cláusula 12.

Subcapa ERP PLCP

Esta sublcáusula proporciona un procedimiento de convergencia para la capa física (PLCP) de la ERP. El procedimiento de convergencia especifica cómo los PSDU's son convertidos en PPDU's para el transmisor y receptor. El PPDU es formado durante la transmisión y se logra a través de la adición del PSDU al preámbulo y encabezado ERP PLCP.

## Formato del PPDU

Una STA en modo ERP deberá soportar tres diferentes formatos de preámbulos y encabezados. El primero de ellos es el preámbulo y encabezado largo (que está basado en el descrito en la cláusula 18.2.2.1 del Estándar 802.11b). Este PPDU proporciona interoperabilidad con las STA's que operan según la cláusula 18 cuando se emplean las tasas de 1, 2, 5.5 y 11 Mbps; el segundo formato es el DSSS – OFDM opcional, que funciona en todas las tasas de transmisión definidas para OFDM y el tercer formato corresponde al ERP – PBCC que opera en todas las tasas de transmisión definidas para dicho esquema de modulación.

## Formato Largo del Preámbulo del PPDU

La figura 3.14 muestra el formato básico para el preámbulo largo del PPDU. Este preámbulo es apropiado para el uso de las siguientes tasas: 1, 2, 5.5 y 11 Mbps (cláusula 18) y es compatible con los BSS's que soportan estos modos. Para emplear los modos opcionales incluidos en la ERP, el preámbulo largo PPDU sólo difiere del descrito en la cláusula 18 en lo siguiente:

A. El uso de un bit en el campo SERVICE que indica cuando el modo opcional ERP – PBCC está siendo utilizado.
B. El uso de dos bits adicionales en el campo SERVICE para resolver la ambigüedad cuando los modos ERP – PBCC a 22 Mbps 33 Mbps están siendo utilizados.

Tres bits del campo SERVICE han sido definidos para soportar los modos opcionales del estándar ERP. La tabla 3.13 muestra gráficamente la asignación de dichos bits dentro del campo SERVICE. Los bits b0, b1, y b4 están reservados y deberán contener el valor de 0. El bit b2 es empleado para indicar la frecuencia de transmisión y los símbolos de reloj que son derivados del mismo oscilador. Para todos los sistemas, el bit de bloqueo del reloj deberá contener el valor de 1. El bit b3 es empleado para indicar si los datos están modulados bajo el esquema ERP – PBCC. Los bits b5, b6, y b7 son empleados para resolver las ambigüedades del campo LENGHT para los modos opcionales ERP – PBCC a 11, 22 y 33 Mbps. Los bits b3, b5 y b6 contienen el valor de 0 cuando se emplea el esquema de modulación CCK.

| b0 | b1 | b2 | b3 | b4 | b5 | b6 | b7 |
|---|---|---|---|---|---|---|---|
| Reserved | Reserved | Locked Clock Bit 0 = not locked 1 = locked | Modulation Selection 0 = Not ERP-PBCC 1 = ERP-PBCC | Reserved | Length Extension Bit (ERP-PBCC) | Length Extension Bit (ERP-PBCC) | Length Extension Bit |

Tabla 3.13
*Asignación de Bits en el campo SERVICE del PPDU 802.11g*

## Formato Corto del Preámbulo del PPDU

La figura 3.15 muestra el formato básico para el preámbulo corto PPDU. Para la ERP, es obligatorio el soporte de este preámbulo. El preámbulo corto es apropiado para los modos a 2, 5.5 y 11 Mbps. Los bits del campo SERVICE y RATE son los mismos que los descritos en el párrafo anterior.

## Formato ERP-OFDM PPDU

El formato, preámbulos y encabezados para el OFDM PLCP PPDU son los que se describen el las cláusulas 17.3.2 hasta la 17.3.5 (las mismas que el estándar 802.11a).

## Formato PPDU de preámbulo largo DSSS-OFDM

El formato de éste preámbulo contiene la misma información que se describió en la sección anterior. La figura 3.14 muestra el formato del PPDU para el caso del preámbulo largo. Como puede apreciarse, el PSDU es anexado la preámbulo PLCP y al encabezado PLCP. El preámbulo PLCP es el mismo que se describe en la cláusula 18.2.3.2 (estándar 802.11b).

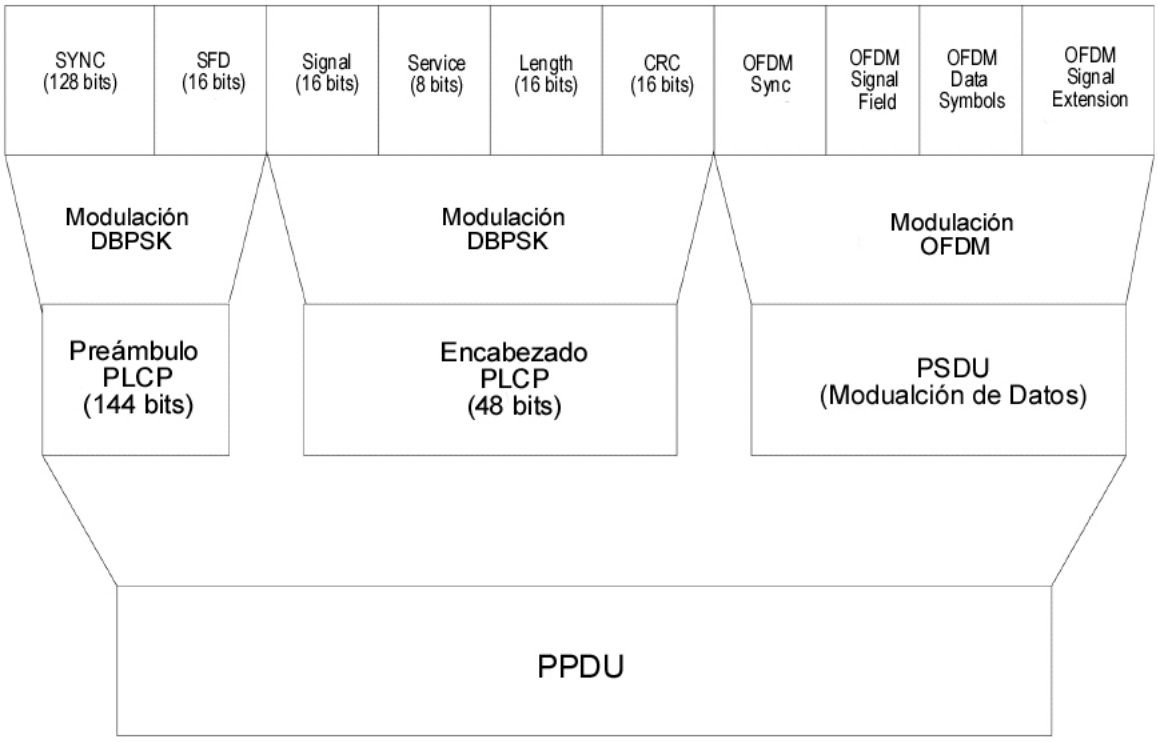



Figura 3.14
*Formato PPDU Largo*
*para el Esquema DSSS-OFDM*

El encabezado PLCP es similar al descrito en la cláusula 19.3.2.1 (802.11g). El PSDU tiene un formato que es idéntico al descrito en el estándar 802.11a. Las diferencias ya fueron descritas en la sección anterior.

## Formato PPDU de preámbulo Corto DSSS-OFDM

El preámbulo corto PLCP y el encabezado son empleados para maximizar la tasa de transmisión neta, reduciendo el sobre-encabezado asociado con el preámbulo y el encabezado. La figura 153B muestra el formato de preámbulo corto PLCP PPDU.

Como puede apreciarse, el PSDU es anexado la preámbulo PLCP y al encabezado PLCP. El preámbulo PLCP es el mismo que se describe en la cláusula 18.2.3.8 y 18.2.3.9 (estándar 802.11b). El encabezado PLCP es similar al descrito en la cláusula 19.3.2.4 (802.11g). El PSDU tiene un formato que es idéntico al descrito en el estándar 802.11a. Las diferencias ya fueron descritas en la sección anterior.

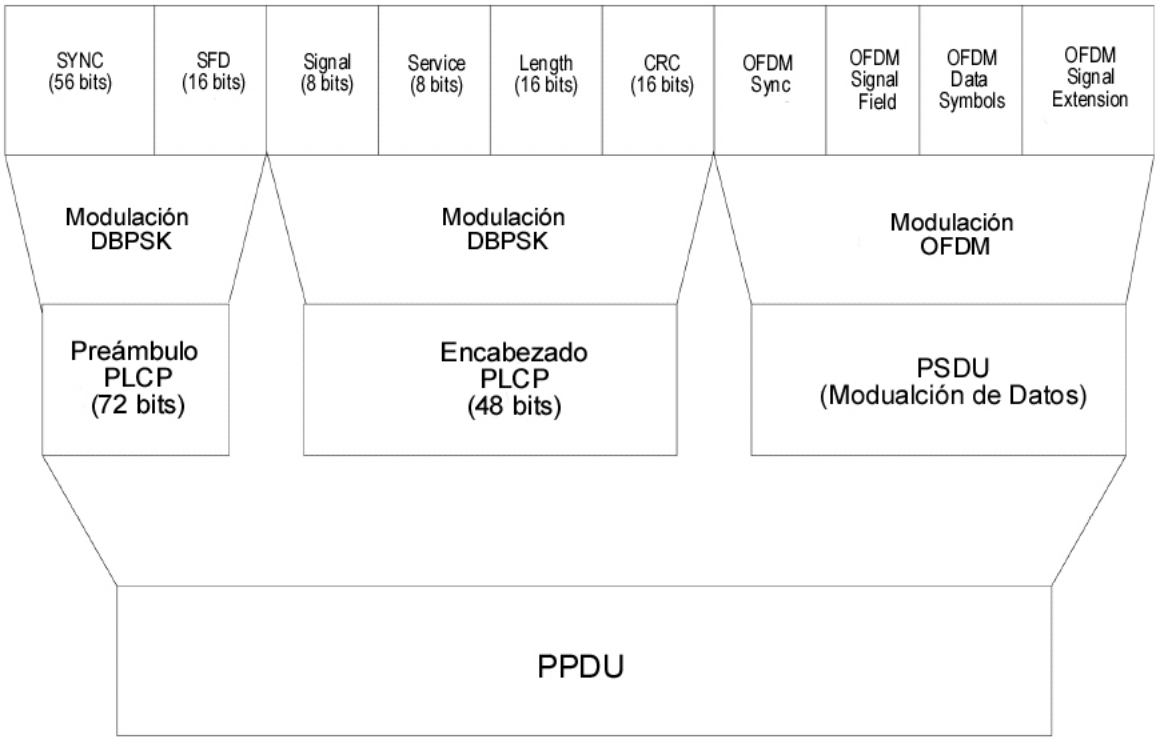



Figura 3.15
*Formato PPDU Corto*
*para el Esquema DSSS-OFDM*

## Panorama del proceso de codificación del PLCP PSDU DSSS-OFDM

Esta subcláusula contiene las definiciones y procedimientos para formar la porción PSDU del PLCP DSSS-OFDM. La figura 3.16 muestra una vista amplificada del mismo. El PSDU se compone de cuatro secciones principales. La primera de ellas es la secuencia larga de sincronización y prueba, que es empleada para la adquisición de los parámetros que requiere el demodulador de OFDM. La segunda parte consiste en el campo OFDM SIGNAL; este campo provee al demodulador de la infomación acerca de la tasa de transmisión y la longitud del campo OFDM que contiene los datos. Después se encuentra el campo de datos y finalmente, aparece el campo SIGNAL EXTENSION, que consiste en un periodo de no transmisión y que se describe con mayor detalle en la sección 19.3.3.4.5.

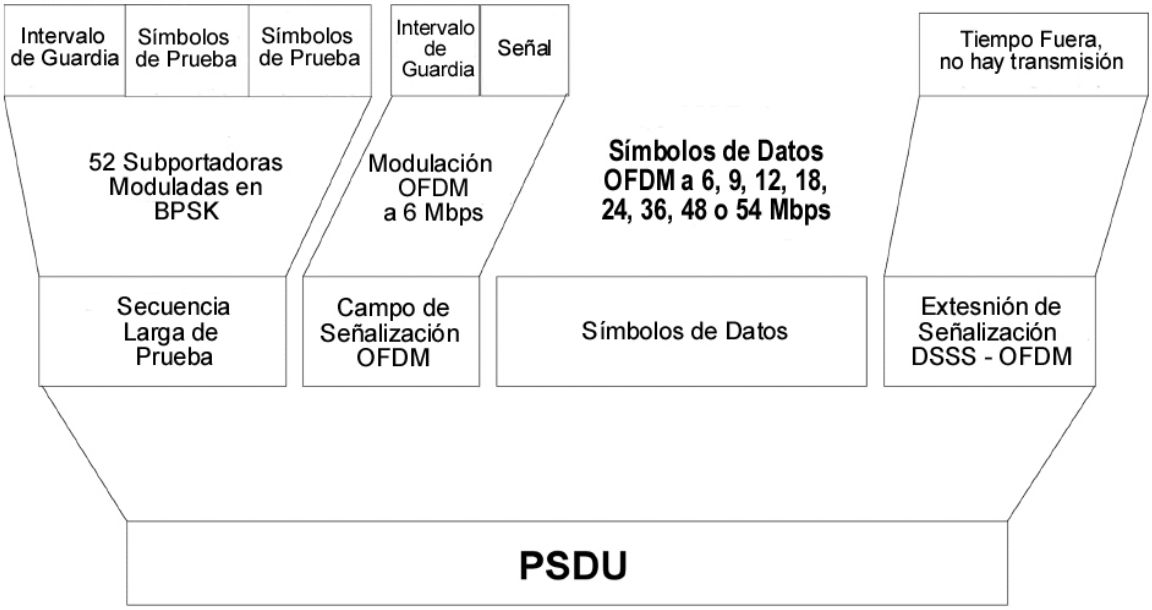



Figura 3.16
*Formato PSDU para el Esquema DSSS-OFDM*

## Especificaciones de Operación de la ERP

Esta subcláusula describe las especificaciones de recepción de la subcapa PMD. Estas especificaciones están definidas en la cláusula 17.3.10 para el modo de operación ERP – OFDM, con excepción del nivel de señal máximo de entrada en el receptor (17.3.10.4). Para el modo ERP – DSSS las especificaciones son las descritas en la cláusula 18.4.8 con excepción del nivel de señal máximo de entrada en el receptor.

- ✓ **Nivel de Sensitividad Mínima en la entrada del Receptor**: La tasa de error en paquetes (PER)[34] del modo de operación ERP – OFDM debe ser menor al 10 % en un PSDU de longitud de 1000 bytes para los niveles de entrada establecidos en la tabla 91 de la cláusula 17.3.10. Los niveles de entrada son específicos para cada tasa de transmisión y se deben medir en los conectores de las antenas. Se asume una figura de ruido (NF)[35] de 10 dB una pérdida por implementación de 5 dB. La PER para los modos ERP – DSSS se especifican en la cláusula 18.4.8.1.

[34] Packet Error Rate
[35] Noise Figure

**Para el Modo de Operación del Modo ERP – PBCC:**

Este modo opcional proporciona a los sistemas la habilidad de manejar tasas de transmisión de 22 y 33 Mbps que son completamente compatibles con los BSS especificados en las cláusulas 15 y 18 y no requieren mecanismos adicionales de coordinación o protección. Además, el modo ERP – PBCC a 22 Mbps es espectralmente idéntico al BSS especificado en la cláusula 18. Se especifican cuatro formatos de modulación ERP – PBCC que trabajan en las siguientes tasas de transmisión: 5.5, 11, 22 y 33 Mbps. En el capítulo anterior se describe como trabajan las tasas de 5.5 y 11 Mbps.

- ✓ **Nivel de Sensibilidad Mínima en la entrada del Receptor**: Para el modo ERP – PBCC, el FER debe ser menos a $8x10^{-2}$ en un PSDU de longitud igual a 1024 octetos para un nivel de entrada de 76 dBm medidos en el conector de la antena. Para el modo ERP – PBCC a 33 Mbps el nivel correspondiente es de 74 dBm.

**Para el Modo de Operación del modo DSSS – OFDM:**

Este modo opcional proporciona a los sistemas la habilidad de emplear el esquema OFDM de manera que sea completamente compatible con los BSS especificados en las cláusulas 15 y 18, sin requerir de coordinación adicional, es decir, no necesita de mecanismos de protección.

La capacidad descrita en esta subcláusula se denomina DSSS – OFDM. Esta ERP complementa al modo de operación del sistema OFDM descrita en la cláusula 19, combinando la modulación en OFDM con los preámbulos del esquema DSSS. Como resultado, el formato del PPDU descrito en la cláusula 18.2.2 permanece relativamente sin cambio para el sistema DSSS – OFDM. El cambio más significativo es el formato del PSDU. El PSDU de portadora unitaria descrito en la clausula 18 es reemplazado por un PSDU que es muy similar a los PSDU's descritos en la cláusula 17. Esta subcláusula marca la diferencia. Además, la cláusula 19.7.2 especifica el comportamiento de la capa física en la transición entre el preámbulo de símbolos modulados con la secuencia Barker y los datos modulados en OFDM para los PSDU's.

CAPÍTULO CUATRO

# Subcapa de Control de Acceso al Medio (MAC)

## 4.1 Panorama de los Servicios MAC

La subcapa MAC es la responsable de la asignación de los procedimientos para el canal, direccionamiento de las unidades de datos de protocolo (PDU), formateo de los frames, detección de errores, fragmentación y re-ensamblado de los frames. El medio de transmisión puede operar en el modo de contención de forma exclusiva, requiriendo que cada una de las estaciones asociadas espere a que el medio esté disponible para la transmisión de cada paquete.

También es responsable de los servicios de seguridad y de administrar el mecanismo WEP[1]. Éste servicio de privacidad consiste en limitar el intercambio de datos entre las estaciones mediante la encriptación de los MSDU's. Para propósitos del estándar, el mecanismo WEP está considerado como un servicio lógico alojado dentro de la subcapa MAC. De hecho, las implementaciones del WEP son transparentes para la subcapa LLC[2] y capas superiores.

Los servicios de seguridad proporcionados por el WEP son los siguientes:

- ✓ Confidencialidad
- ✓ Autenticación
- ✓ Control de acceso en conjunto con la administración de capa.

Por último, los servicios proporcionados por la subcapa MAC permiten y en ciertos casos requieren el reordenamiento de los MSDU's. La MAC no reordena los MSDU's de manera intencional excepto cuando se requiere para mejorar la probabilidad de entrega exitosa basada en el modo de operación actual (administración de potencia) de las estaciones receptoras asignadas.

El único efecto de este reordenamiento (si es que hay alguno) para el conjunto de MSDU's recibidos en la interfase de los servicios MAC, es el cambio en el orden de entrega de los MSDU's de *broadcast* y *multicast.*

[1] Wired Equivalent Privacy. Este mecanismo se estudia a detalle en el próximo capítulo.
[2] Logical Link Control, subcapa de la capa 2 del modelo OSI.

Para optimizar la transmisión de los MSDU's, el medio puede alternar entre dos modos de contención, conocidos como el periodo de contención (CP)[3] y el periodo de contención libre (CFP)[4]. Cuando se encuentra operando el CFP, el medio empleado es controlado (o mediado) por el AP; de esta manera se descarta que las estaciones se encuentren en modo de contención.

El Estándar 802.11 soporta tres diferentes tipos de frames: de administración, de control y de datos. Los frames de administración son empleados para la asociación y *de-asociación* de las estaciones con los AP's, sincronización, autenticación y *de-autenticación*. Los frames de control son empleados para el reconocimiento y confirmación de recepción durante el CP, y para la finalización de un CFP. Los frames de datos son empleados para transmitir datos durante el CP y el CFP.

El mínimo intercambio de los frames del protocolo MAC consiste en dos frames, un frame enviado por la estación origen hacia la destino, y un frame de verificación de la estación destino que indica que el frame fue recibido correctamente. Si la estación origen no recibe este frame de verificación, tratará de re-transmitir la información de acuerdo al procedimiento descrito a continuación. Este procedimiento reduce la tasa de error inherente en el medio a expensas del consumo adicional del ancho de banda, pero sin la necesidad de recurrir a los protocolos de capas superiores, ya que los tiempos fuera de éstos son medidos en segundos y por ello, resulta más eficiente tratar este asunto desde la subcapa MAC.

### 4.1.1 El Problema del Nodo Oculto

Este problema no ocurre en una LAN cableada y es el principal problema de las redes inalámbricas. Aunque posteriormente se analizará en el capítulo 6, en el presente subtema nos servirá para ejemplificar el mecanismo de operación CSMA/CA. De acuerdo a los rangos de transmisión de las estaciones A y C de la siguiente figura, no es posible que una pueda escuchar a la otra, por lo que si ambas estaciones transmiten al mismo tiempo hacia la estación B, los frames enviados se colisionarán.

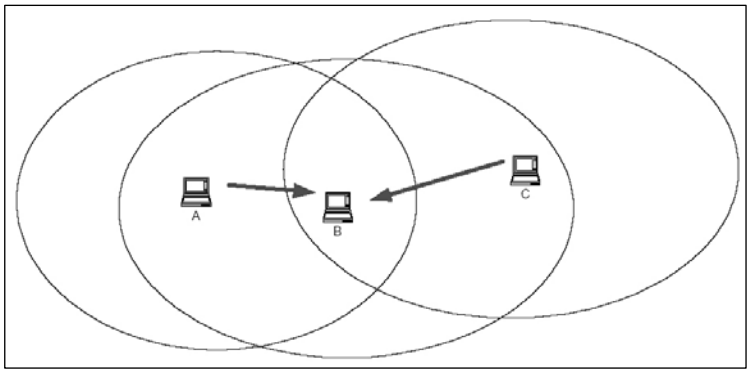



Figura 4.1
*El problema del Nodo Oculto*

[3] Contention Period
[4] Contention Free Period

El protocolo de intercambio de frames del Estándar 802.11 agrega dos frames adicionales: RTS[5] (Solicitud de transmisión) y CTS[6] (Libre para Transmitir). La estación origen envía el RTS y la estación receptora envía el CTS; los demás nodos que reciban estos frames, suspenderán sus transmisiones por un periodo específico determinado dentro de los frames CTS/RTS. En otras palabras, las estaciones que escuchan el frame RTS retrasan su transmisión hasta que reciben el CTS de la estación destino. Si existe otra estación que requiere transmitir y no recibe el CTS, empezará a transmitir. De nueva cuenta, si una estación adicional requiere comenzar una transmisión, tendrá que esperar la confirmación del frame CTS producido por la estación que esté transmitiendo actualmente.

En la estación origen, una falla en el protocolo de intercambio implica la retransmisión de los datos. Esto es tratado como una colisión y las reglas para distribuir las retransmisiones serán tratadas más adelante. Para prevenir que el mecanismo de retransmisión intente la entrega reiterada de un solo frame, existen contadores y temporizadores que limitan el tiempo de vida de los frames.

El mecanismo RTS/CTS puede ser desactivado por un atributo en la base de información administrativa (MIB). Resulta práctico desactivar dicha función en los siguientes casos:

- Cuando haya una baja demanda del ancho de banda
- Cuando las estaciones se encuentren ubicadas en un área donde cada una de las estaciones pueda escuchar a las demás estaciones asociadas.
- Donde no exista demasiada contención para el canal.

## 4.2 Mecanismo Básico de Acceso

El mecanismo básico de acceso es el Acceso Múltiple con Sensor de Portadora / Prevención de Colisión (CSMA/CA)[7], que contiene un *backoff* exponencial similar al que se maneja en el Estándar 802.3 con algunas diferencias significativas. CSMA/CA es un mecanismo de acceso que "escucha antes de transmitir". Cuando hay una transmisión en el medio, la estación no comenzará a transmitir su propia información. Si existiera una colisión y la transmisión sufriera daños, la operación de este mecanismo asegurará la correcta recepción de la información transmitida a través del medio inalámbrico.

Cuando una estación escucha el medio antes de transmitir y detecta que hay una transmisión en progreso, dicha estación entra en un periodo de espera determinado

[5] RTS: Request to Send
[6] CTS: Clear to Send
[7] Carrier Sense Multiple Access / Collision Avoidance

por el *algoritmo binario exponencial.* Este mecanismo selecciona un número aleatorio el cual representa la cantidad de tiempo que se dejará pasar hasta que no haya más transmisiones. El número aleatorio originado por este algoritmo está distribuido de manera uniforme dentro de un rango, llamado *ventana de contención.* El tamaño de este número se duplica cada vez que el intento de transmisión es rechazado y así, el rango es reducido hasta que dicho número es rechazado por el rango especificado. Una vez que la transmisión es exitosa, el rango se reduce a un valor mínimo para la próxima transmisión.

Es extremadamente inusual que un dispositivo inalámbrico sea capaz de transmitir y recibir de manera simultánea; el Estándar 802.11 emplea la prevención de colisiones en lugar de la detección de colisiones ejecutada por el Estándar 802.3. También es inusual que todos los dispositivos de una WLAN se puedan comunicar directamente entre ellos. Por esta razón la capa MAC de este estándar implementa el vector de distribución de la red (NAV)[8]. El NAV es un valor que le indica a una estación la cantidad de tiempo que resta para que el medio vuelva a quedar libre. Incluso si el medio no parece tener alguna transmisión en proceso, la estación puede evitar transmitir su información. Entonces, el NAV actúa como un mecanismo sensor de portadora virtual.

El protocolo básico de la capa MAC 802.11 es la función DCF[9], basada en CSMA. Las estaciones entregan MSDU's. Estos MSDU's de longitud arbitraria (hasta 2304 bytes) son transmitidos hasta que no existe otra transmisión en progreso que ocupe el canal. Sin embargo, si dos estaciones detectan al mismo tiempo que el canal está libre, ocurrirá una colisión. El Estándar 802.11 define un mecanismo de Prevención de Colisión (Collision Advoidance) para reducir la probabilidad de dichas colisiones. Antes de comenzar una transmisión, una estación tiene que seguir monitoreando el canal por un tiempo adicional después de detectar que el canal está sin actividad; esta duración mínima corresponde al DIFS[10], el cual tiene una duración de 34 μs para el Estándar 802.11a, por ejemplo. Únicamente si el canal continúa sin actividad durante este intervalo de tiempo, se le permitirá a la estación comenzar a transmitir.

En resumen:

1. Cuando la capa MAC recibe una petición para la transmisión de un frame, se lleva acabo la verificación del medio de manera física y virtual a través de los mecanismos descritos.
2. Si el medio no está ocupado por un intervalo DIFS (o un EIFS si es que el frame recibido previamente contenía errores), la capa MAC comenzará la transmisión del frame.

[8] Network Allocation Vector
[9] Distributed Coordination Function; ésta función se detalla en la sección 4.4.2
[10] Tanto el DIFS como el EIFS serán definidos en la siguiente sección.

3. Si el medio se encuentra en uso durante el intervalo DIFS. La capa MAC seleccionará un *backoff* y un incremento en el contador de reintentos.
4. La capa MAC decrementará el valor del backoff cada vez que se detecte que el medio se encuentra sin actividad para el intervalo de una ranura de tiempo.
5. Si ocurre una colisión, la ventana de contención se duplica y se selecciona un nuevo intervalo de backoff.

Un ejemplo de la operación de la DCF se muestra en la siguiente figura:

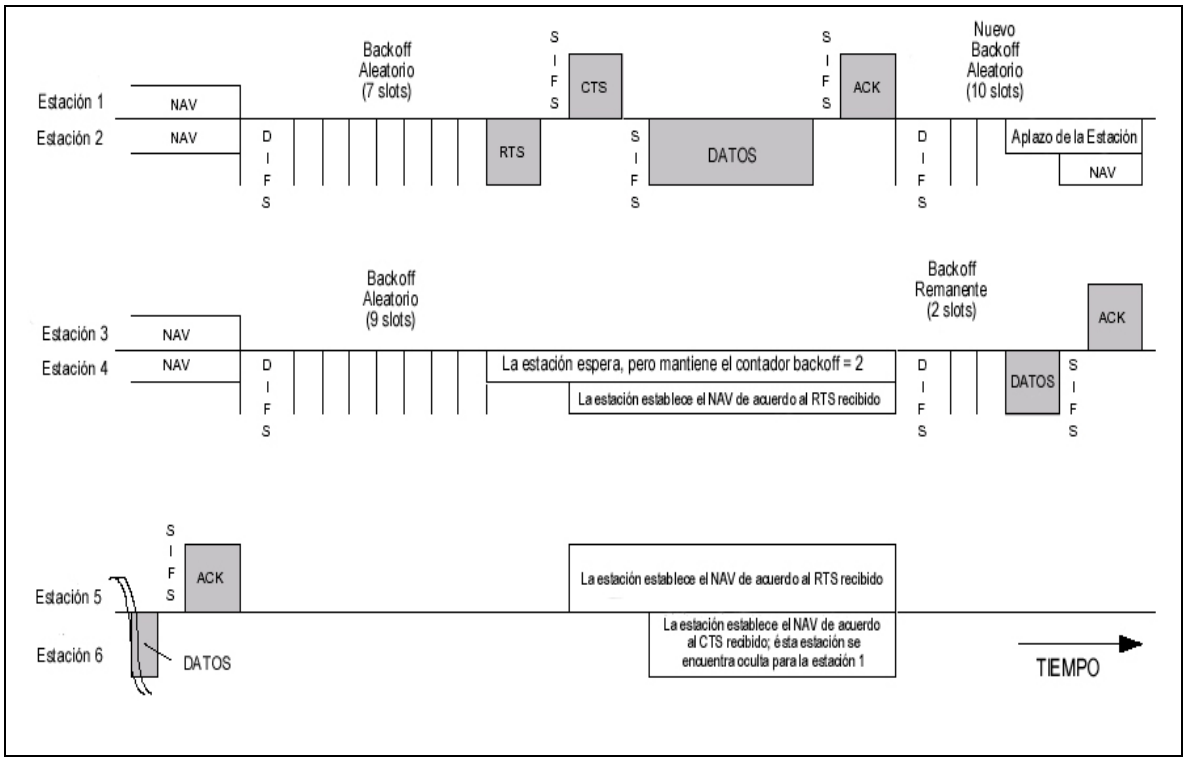



Figura 4.2
*Esquema de operación de la DCF*

## 4.3 La subcapa MAC en el Estándar IEEE 802.11

### 4.3.1 Formato General del Frame

Los MPDU's del protocolo MAC o los frames de la subcapa MAC son descritos como una secuencia de campos en un orden específico.

El formato del frame comprende un conjunto de campos que se presentan en un orden determinado en todos los frames. La figura 4.3 muestra esta estructura en general.


Figura 4.3
*Formato General del Frame MAC 802.11*

Los campos Dirección 2, Dirección 3, Secuencia de Control, Dirección 4, Cuerpo del Frame se presentan en cierto tipo de frames. Cada uno de estos campos es definido en la cláusula 7.1.3. El formato de cada frame individual se define en la cláusula 7.2. A continuación se describe cada uno de los campos del Formato General.

## Control del Frame

Este campo consiste en los siguientes subcampos: Versión del protocolo, Tipo, Subtipo, DS destino, DS origen, Más fragmentos, Reintento, Administración de Potencia, Más datos, WEP y Orden.

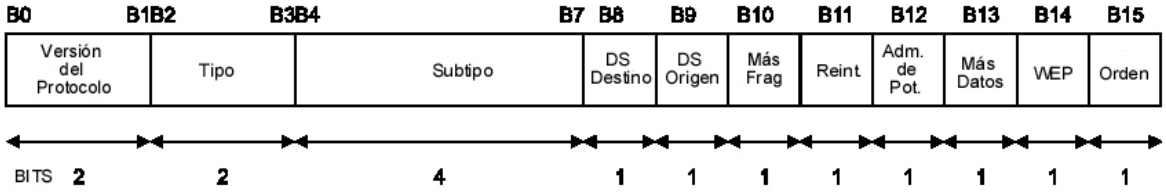



Figura 4.4
*Formato del sub-campo*
*Control del Frame*

**Versión del Protocolo:** Tiene longitud de 2 bits. El valor para este estándar es de 0. Cuando se recibe un frame con un valor distinto, será descartado sin enviar la notificación a la estación emisora o a la LLC.

**Tipo y Subtipo:** Identifican la función del frame. Existen tres tipos de frame: Control, Datos y Administración. En la siguiente tabla 4.1 se muestran las combinaciones válidas para estos campos.

**DS Origen y Destino:** Tiene el valor de 1 para los frames que contienen DS (secuencia directa) y se incluye para todas las estaciones asociadas con el AP. En otros tipos de frames, el valor es 0.

**Más Fragmentos:** Tiene el valor de 1 para los frames de tipo datos o administración que contienen fragmentos del MSDU que se esté enviando. Para los demás tipos de frame, el valor es 0.

**Reintento:** El valor será de 1 en los frames de datos o administración que son producto de una retransmisión o de un frame transmitido con anterioridad. En los otros frames el valor es 0. Una estación receptora emplea esta información para auxiliar al proceso de eliminación de frames duplicados.

| **Tipo** b1b2 | **Tipo** Descripción | **Subtipo** b7b6b5b4 | **Subtipo** Descripción |
|---|---|---|---|
| 00 | Administración | 0000 | Petición de asociación |
| 00 | Administración | 0001 | Respuesta de asociación |
| 00 | Administración | 0010 | Petición de re-asociación |
| 00 | Administración | 0011 | Respuesta de re-asociación |
| 00 | Administración | 0100 | Petición de "encuesta" |
| 00 | Administración | 0101 | Respuesta de "encuesta" |
| 00 | Administración | 0110-0111 | Reservado |
| 00 | Administración | 1000 | Beacon |
| 00 | Administración | 1001 | ATIM |
| 00 | Administración | 1010 | De-asociación |
| 00 | Administración | 1011 | Autenticación |
| 00 | Administración | 1100 | De-autenticación |
| 00 | Administración | 1101-1111 | Reservado |
| 01 | Control | 0000-1001 | Reservado |
| 01 | Control | 1010 | Latencia (power save) |
| 01 | Control | 1011 | Petición para transmitir (RTS) |
| 01 | Control | 1100 | Libre para Transmitir (CTS) |
| 01 | Control | 1101 | Verificación (ACK) |
| 01 | Control | 1110 | Libre de contención (CF)-Fin |
| 01 | Control | 1111 | CF-Fin + CF-ACK |
| 10 | Datos | 0000 | Datos |
| 10 | Datos | 0001 | Datos + CF-ACK |
| 10 | Datos | 0010 | Datos + CF-Encuesta (poll) |
| 10 | Datos | 0011 | Datos + CF-ACK + CF-poll |
| 10 | Datos | 0100 | Función nula (sin datos) |
| 10 | Datos | 0101 | CF-ACK (sin datos) |
| 10 | Datos | 0110 | CF-poll (sin datos) |
| 10 | Datos | 0111 | CF-ACK + CF-poll (sin datos) |
| 10 | Datos | 1000-1111 | Reservado |
| 11 | Reservado | 0000-1111 | Reservado |

Tabla 4.1
*Combinaciones válidas para la Identificación del Frame*

**Administración de potencia:** Se emplea para indicar el modo de administración de potencia de las estaciones. El valor de este campo permanece constante para una estación particular dentro de una secuencia de intercambio. El valor indica el modo en el cual se debe encontrar la estación después de completarse la secuencia de intercambio de frames. El valor de 1 indica que la estación estará en el modo de ahorro de energía. El valor de 0 indica que se encuentra en el modo activo. Este valor siempre es 0 en los frames transmitidos por los AP's.

**Más datos:** El campo es empleado para indicarle a una estación que se encuentra en el modo de ahorro de energía, que hay más MPDU's en cola dirigidos a dicha estación en el AP. Un valor de 1 indica que hay al menos un MSDU en cola. El campo tendrá un valor de 0 en los frames broadcast/multicast transmitidos por el AP cuando no existan mas MSDU's broadcast/multicast remanentes a ser transmitidos por el AP durante el intervalo de transmisión del frame bacon y en todos los frames broadcast/multicast transmitidos por las estaciones que no son AP.

**WEP:** Tiene el valor de 1 cuando el campo Cuerpo del Frame contiene información que ha sido procesada por el algoritmo WEP. El campo WEP solo tendrá dicho valor dentro de los frames tipo Datos o Administración (subtipo autenticación). El valor será 0 en cualquier otro tipo de frames.

**Orden:** Contiene el valor de 1 cuando el tipo de frame es Datos y contiene un MSDU o un fragmento, el cual está siendo transferido mediante la clase de servicio *Strictly Ordered*. El campo tiene valor de 0 en cualquier otro caso.

Duración/ID

El contenido de este campo es como sigue:

A) En los frames tipo control, del subtipo ahorro de energía (PS-poll), el contenido de este campo contiene la información de identidad de asociación (AID)[11] de la estación que transmite el frame. El valor del AID se encuentra en el rango de 1-2007.
B) En los demás tipos de frames, este campo contiene una duración variable como se describe en la cláusula 7.2. Para frames transmitidos durante el

[11] Association Identity

periodo libre de contención, la duración del campo se establece en 32 768. Siempre que el contenido del campo Duración/ID es menor a 32 768, el valor de la duración es empleado para actualizar el vector de distribución de la red de acuerdo a los procedimientos definidos en la cláusula 9.

Direcciones

Estos campos son empleados para reconocer el identificador de la BSS (BSSID), dirección destino (DA)[12], dirección origen (SA), dirección de la estación transmisora (TA) y dirección de la estación receptora (RA). Algunos campos de direcciones son usados de manera específica de acuerdo a la posición relativa dentro del encabezado MAC (1 - 4), independientemente del tipo de direcciones que se presenten en ese campo. Por ejemplo, para corroborar la dirección del receptor, siempre se realiza sobre el contenido del campo Dirección 1 en los frames recibidos; y por otro lado, las direcciones del receptor de los frames CTS y ACK siempre se obtienen del contenido del campo Dirección 2 en el frame CTS correspondiente o del frame que está siendo confirmado.

- **Representación de la Dirección**

Cada campo de dirección contiene una dirección de 48 bits tal y como se especifica en el Estándar 802 (edición 1990).

- **Asignación de las Direcciones**

1. Dirección Individual: es la dirección asociada con una estación particular de la red.
2. Dirección de Grupo: es una dirección multi-destinatario, asociada con una o más estaciones de una red dada. Los dos tipos de direcciones grupales son:

   2.1 Dirección de grupo-multicast: es una dirección asociada por convención de un nivel superior con un grupo de estaciones lógicamente relacionadas entre sí.

   2.2 Dirección broadcast: consisten en direcciones multicast predefinidas que siempre denotan a un conjunto de estaciones de una LAN dada. Todos los 1's en el campo dirección destino (DA) se interpretan como direcciones de broadcast. Este grupo es definido por cada medio de comunicación que consiste en todas las estaciones activas que se encuentran conectadas en dicho medio. Todas las estaciones son capaces de reconocer las direcciones de broadcast.

[12] DA: Destination Address; SA: Source Address;
RA: Receiver Address; TA: Transmission Address.

- **Campo BSSID**

Este campo contiene 48 bits con el mismo formato que la dirección MAC definida en el Estándar 802. Este campo únicamente identifica a cada BSS. El valor de este campo, en una infraestructura BSS, es la dirección MAC que está siendo usada por una estación en un AP de la BSS. Cuando el campo contiene únicamente 1's, significa que es un frame de tipo broadcast BSSID.

## Secuencia de Control

Este campo tiene una longitud de 16 bits y consiste en dos subcampos: Número de Secuencia y Número de Fragmento.

**Número de Secuencia:** Es de longitud de 12 bits indicando el número que le corresponde a un MSDU o MMPDU dentro de la secuencia de transmisión. Es decir, cada MSDU transmitido por la estación tiene asignado un número dentro de una secuencia. Éstos números se asignan de un contador unitario de módulo 4096, comenzando desde el 0 e incrementándose en 1 para cada MSDU o MMPDU. El valor de este campo se mantiene constante durante las retransmisiones de cualquier tipo.

**Número un de Fragmento:** Contiene 4 bits indicando el número de cada fragmento de MSDU o MMPDU.

## Cuerpo del Frame

Este campo de longitud variable que contiene información específica de los tipos y subtipos de los frames individuales. El tamaño mínimo es de 0 octetos. El tamaño máximo se define por la longitud máxima (MSDU+ICV+IV), donde ICV y IV son campos del mecanismo WEP.

## Campo FCS

Este campo contiene 32 bits resultantes del código de redundancia cíclica (CRC)[13]. El FCS es calculado sobre todos los campos del encabezado MAC y del cuerpo del frame. A ellos se les denomina campos de cálculo.

[13] Cyclic Redundancy Code

El FCS se calcula mediante el siguiente generador polinomial de grado 32:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

El FCS es el complemento de los 1's de la suma de lo siguiente:

a) El residuo de $x^k \times (x^{31} + x^{30} + x^{29} + ...x^2 + x + 1)$ dividido (en módulo 2) por G(x), donde *k* es el número de bits en los campos de cálculo y

b) El residuo después de la multiplicación de los contenidos (tratados como polinomios) de los campos de cálculo por $x^{32}$ y posteriormente dividido por G(x).

El FCS se transmite comenzando con los términos de mayor orden. En una implementación típica, en el transmisor, el residuo inicial de la división se establece que todos los términos sean 1's y después son modificados por la división de los campos de cálculo del generador polinomial G(x). Después, se transmiten los complementos de los 1's de este residuo.
En el receptor, el residuo inicial se establece de manera que todos los valores sean 1's. Si la entrada de bits en serie de los campos de cálculo y el FCS cuando se divide por G(x) da como resultado un residuo distinto de cero, entonces significa que no hay errores en la transmisión. El único residuo que debe existir es el siguiente polinomio:

$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

El detalle de cada uno de los subtipos de frame existentes (Control, RTS, CTS, ACK, CF-end, ACK, PS-Poll, Datos, Administración, Control, Beacon, IBSS, Asociación, Deasociación, Autenticación, Deautenticación, etc.) se encuentra ampliamente descrito en la sección 7.2 del Estándar 802.11 – 1999.

### 4.3.2 Formatos Específicos de Frames

Frame RTS

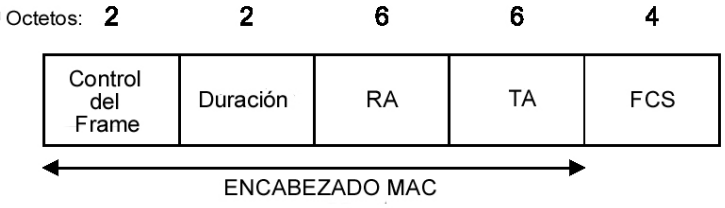



Figura 4.5
*Formato Frame RTS*

El campo RA de este tipo de frame, se refiere a la dirección de la STA dentro del medio inalámbrico (WM). En el campo TA está contenida la dirección de la STA que está transmitiendo el frame RTS.

El valor del campo duración representa, en microsegundos, el tiempo requerido para transmitir los frames de datos o de control además del frame CTS, el frame ACK y los tres intervalos SIFS.

Frame CTS

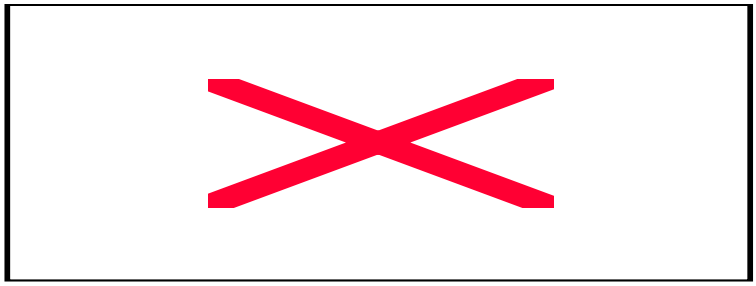


Figura 4.6
*Formato Frame CTS*

El campo RA de este frame es copiado del campo TA del frame RTS enviado previamente, del cual el CTS es su respuesta. El valor del campo Duración se obtiene del mismo campo del frame RTS recibido previamente, menos el tiempo, en microsegundos, que se requiere para transmitir el frame CTS y su intervalo SIFS.

Frame de Confirmación (ACK)

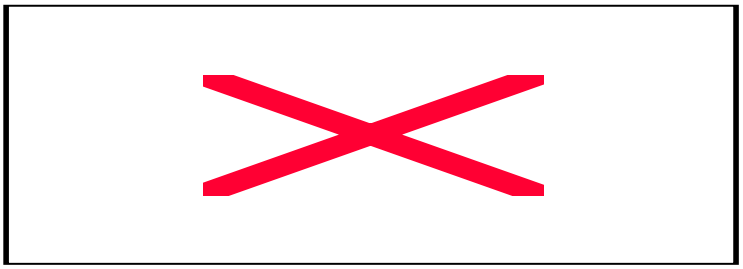


Figura 4.7
*Formato Frame ACK*

El campo RA del frame ACK es copiado del campo Address 2 del frame previamente recibido: datos, administración o PS-Poll frame.

Los demás tipos de frame PS-Poll, CF-End, CF-End + CF-ACK son descritos a detalle en las cláusulas 7.2.1.4 a la 7.2.1.6 del Estándar 802.11.

## Frames de Datos

El formato del frame de datos es independiente de sus subtipos y es el que se muestra a continuación:


Figura 4.8
*Formato Frame de Datos*

El contenido de los campos Dirección de los frames de datos depende de los valores de DS destino (*To DS*) y DS origen (*DS From*) contenidos en el frame de control y que tienen la relación que se muestra en la siguiente tabla. Cuando el contenido del campo se encuentra en N/A, dicho campo es omitido. Hay que notar que el campo Dirección 1 siempre mantiene la dirección del receptor, y que el campo Dirección 2 siempre mantiene la dirección del la estación que está transmitiendo el frame.

| DS Destino | DS Origen | Dirección 1 | Dirección 2 | Dirección 3 | Dirección 4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | N/A |
| 0 | 1 | DA | BSSID | SA | N/A |
| 1 | 0 | BSSID | SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |

Tabla 4.2
*Combinaciones válidas para el Contenido de los Campos de Direcciones*

De la tabla:

- ✓ DA = *Destination Address*, es la dirección destino del MSDU (o fragmento).
- ✓ SA = *Source Address*, es la dirección de la entidad MAC que originó el MSDU.
- ✓ RA = *Receiver Address*, es la dirección de la STA contenida en el AP en el Sistema de Distribución (DS) del medio inalámbrico, que es el siguiente receptor al que se dirige el frame.
- ✓ TA = *Transmitter Address*, es la dirección de la STA contenida en el AP en el DS del medio inalámbrico, que está transmitiendo el frame.

- ✓ BSSID = *BSS Identifier*, es determinado de la siguiente forma:
  - Si la estación es un AP o se encuentra asociado con un AP, el BSSID es la dirección que actualmente se encuentra en uso por la STA contenida en el AP.
  - Si la estación es un miembro de un IBSS, el BSSID es el BSSID del IBSS.

Las estaciones emplean el contenido del campo *Dirección 1* para llevar a cabo la correspondencia de direcciones par efectos de las decisiones en la recepción. En caso de que dicho campo contenga una dirección de grupo, el BSSID también es validado para asegurar que el frame de broadcast o multicast sea para la misma BSS. Las estaciones emplean el contenido del campo *Dirección 2* para dirigir el frame de confirmación (ACK) en caso de ser necesario.

Dentro de todos los tipos de frames durante el CFP, el valor del campo *Duración* se fija al valor 32 768. Si los frames de datos se transmiten durante un periodo de contención, el valor del campo Duración se establece de acuerdo a las siguientes reglas:

- Si el campo *Dirección 1* contiene una dirección de grupo, el valor se establece en 0
- Si el bit de Más Fragmentos se encuentra en 0 de un frame de control y el campo *Dirección 1* contiene una dirección individual, el valor del campo se establece, en microsegundos, a la cantidad requerida para transmitir el frame ACK con su respectivo SIFS.
- Si el bit de *Más Fragmentos* se encuentra en 1 de un frame de control y el campo *Dirección 1* contiene una dirección individual, el valor del campo se establece, en microsegundos, a la cantidad requerida para transmitir el siguiente fragmento del frame, además de dos frames ACK y tres intervalos SIFS.

El cálculo del valor de la duración para el frame de datos está basado en las reglas de la cláusula 9.6 del Estándar 802.11, que determinan la tasa de transmisión a la cual los frames de control son transmitidos. Todas las estaciones procesan el valor del campo Duración con un valor menor o igual a 32 767 para frames válidos y con la intención de actualizar el NAV bajo las funciones de coordinación correspondientes.

## 4.4 Descripción Funcional de la Subcapa MAC

### 4.4.1 Arquitectura de la capa MAC

Ésta arquitectura, puede describirse de acuerdo a la siguiente figura:

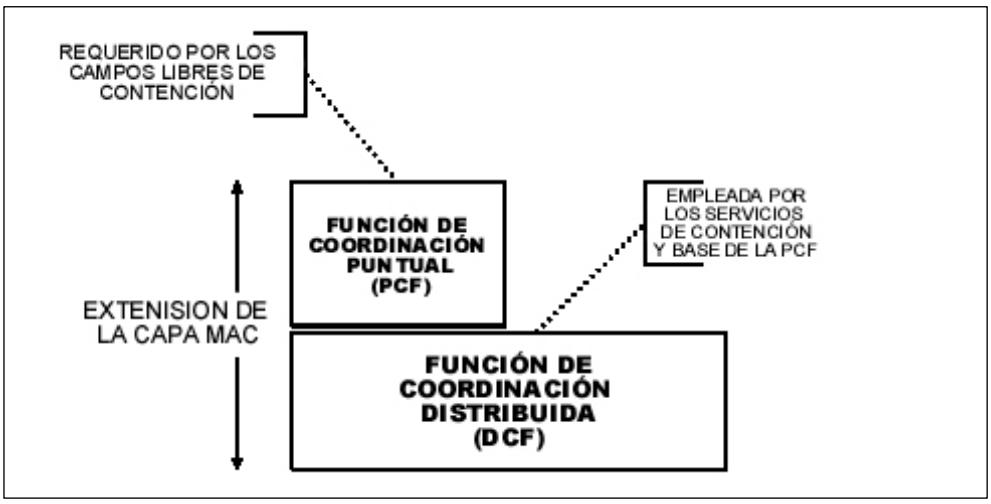



Figura 4.9
*Arquitectura de la Subcapa MAC*

### 4.4.2 DCF

El acceso básico del protocolo es la DCF, que permite compartir el medio de manera automática entre la capa PHY a través del uso del mecanismo CSMA/CA seguido de un tiempo de backoff aleatorio en caso de que el medio se encuentre ocupado. Además, todo el tráfico direccionado emplea una confirmación positiva (ACK frame), donde las retransmisiones son agendadas si no se recibe el frame ACK.

El protocolo CSMA/CA está diseñado para reducir las probabilidades de colisión entre las múltiples STA's que acceden de manera compartida al medio. Justo después de que el medio se encuentre desocupado es cuando existe la mayor posibilidad de que exista una colisión. Esto se debe a que las múltiples STA's pueden estar esperando a que el medio se encuentre disponible de nueva cuenta. El mecanismo sensor de portadora, es llevado a cabo a través de dos mecanismos: uno físico y otro virtual.

El mecanismo virtual de sensor de portadora es llevado a cabo a través del anuncio de la distribución de información de reservaciones, impidiendo de esta manera el uso del medio. El intercambio de los frames RTS y CTS antes del envío de los datos actuales corresponde a una parte de ésta distribución de la información de reservaciones. Dichos frames contienen el campo Duración/ID que define el periodo de tiempo que el medio estará reservado para transmitir el frame actual y el de confirmación. Todas las estaciones dentro del rango de recepción e incluso la estación de origen (la cual transmite el RTS) o la STA destino (la cual transmite el CTS) deberán estar al tanto de las reservaciones del medio.

Si el frame CTS de regreso no es detectado por la STA que originó el RTS, la estación origen deberá repetir el proceso más rápidamente que si el frame completo de datos hubiera sido transmitido y no se hubiera detectado el frame ACK.

### 4.4.3 Mecanismo Sensor de Portadora

Las funciones físicas y virtuales de sensor de portadora se emplean para determinar el estado del medio. Cuando ambas funciones indican que el medio se encuentra ocupado, no es posible acceder a él; en caso contrario se establece que el medio se encuentra inactivo. El mecanismo físico de sensor de portadora debe ser proporcionado por la capa PHY (esta parte se describe de manera amplia en la sección 12 del Estándar 802.11-1999). El mecanismo virtual de sensor de portadora debe ser proporcionado por la capa MAC. Este mecanismo es dirigido por el vector de distribución de la red (NAV). El NAV mantiene una predicción del futuro tráfico del medio basado en la información de la duración que se encuentra en los frames RTS/CTS antes del intercambio de datos. La duración de la información se encuentra disponible en los encabezados MAC de todos los frames enviados durante el CP entre otros frames de control.

El NAV puede ser idealizado como un contador que contiene dos estados: cuando su valor es cero, significa que el medio se encuentra inactivo; cuando es diferente de cero, la indicación es que está ocupado.

La recepción de algunos frames, requieren que las STA's receptoras respondan con una confirmación, generalmente con el frame ACK, si es que el FCS del frame recibido es correcto. Esta técnica es conocida como confirmación positiva. La ausencia en la recepción del frame ACK indica a la estación STA que ha ocurrido un error. Sin embargo, pudiera existir el caso que el frame se ha recibido correctamente pero el error ocurrió en la recepción del frame ACK. Esta situación no puede ser diferenciada de un error en la transmisión de los datos y es necesario retransmitir.

### 4.4.4 Espacios Inter-Frame

El intervalo de tiempo que existe entre los frames se denomina espacio inter-frame (IFS)[14]. Una STA determina que el espacio se encuentra disponible a través del uso de la función de sensor de portadora para un intervalo especificado. Existen cuatro tipos de IFS's que se definen para proporcionar niveles de prioridad para acceder al medio inalámbrico, los cuales se listan a continuación en el orden de menor a mayor duración.

[14] Inter-space Frame

1. El espacio inter-frame corto (SIFS)[15], determinado por la capa PHY
2. El espacio inter-frame de prioridad (PIFS - PCF)[16]
3. El espacio inter-frame distribuido (DIFS - DCF)[17]
4. El espacio inter-frame extendido (EIFS)[18]

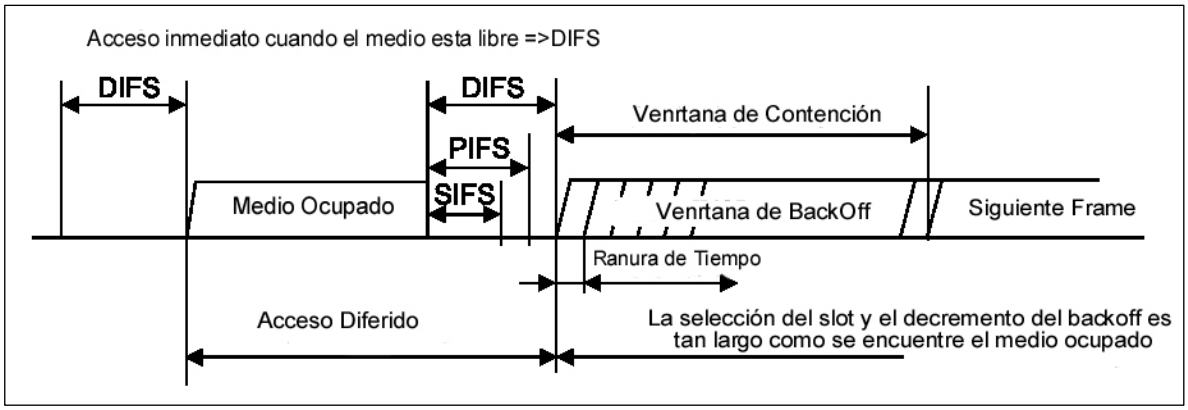



Figura 4.10
*Representación de los espacios Inter-Frame*

Los diferentes IFS's deberán ser independientes de la tasa de transmisión que manejen las STA's.

## IFS Corto (SIFS)

El SIFS deberá ser empleado por los frames ACK, CTS, el segundo MPDU o subsecuente, y por las STA's que responden a la "encuesta" del PCF. El SIFS es el tiempo que transcurre desde el final del último símbolo del frame previo hasta el comienzo del primer símbolo del preámbulo del frame subsecuente Este periodo es el mas pequeño de los IFS's y es empleado cuando las STA's se encuentran utilizando al medio y necesitan mantenerlo ocupado para completar el intercambio de la información. Empleando el espacio más pequeño entre las transmisiones dentro del intercambio de frames, se previene a otras STA's de intentar utilizar al medio, dando prioridad de completar la secuencia de intercambio de frames en progreso.

## IFS de Prioridad (PIFS)

El PIFS debe ser usado únicamente por las STA's que operan bajo el PCF, con el objeto de ganar acceso prioritario al medio durante el CFP. Una STA que emplea el PCF se le debe permitir la transmisión de tráfico libre de contención después de

[15] Short InterFrame Space
[16] Priority InterFrame Space
[17] Distributed InterFrame Space
[18] Extended InterFrame Space

que el mecanismo sensor de portadora determina que el medio se encuentra ocupado. La cláusula 9.3 describe detalladamente el uso de los PIFS en las STA's que operan bajo el PCF.

IFS Distribuido (DIFS)

Los DIFS's son empleados por las STA's que operan bajo el DCF para transmitir frames de datos (MPDU's) y frames de administración (MMPDU's). Una STA que usa la DCF está autorizada para transmitir si el mecanismo sensor de portadora determina que el medio se encuentra ocupado después de que se ha recibido un frame correctamente y su tiempo de backoff ha expirado.

Una STA que emplea el DCF no transmitirá dentro de un EIFS después de determinar que el medio se encuentra ocupado seguido de la recepción del frame que contiene una indicación primitiva (en la parte PHYRXEND) de que ocurrió un error o que el valor del FCS MAC no es correcto. Una estación puede transmitir después de la recepción subsecuente de un frame libre de errores re-sincronizando a la STA. Esto permite a las STA transmitir mediante el empleo del DIFS seguido de dicho frame.

IFS Extendido (EIFS)

El EIFS es empleado por la DCF siempre que la capa PHY le indica a la capa MAC que un frame del cual se ha comenzado su transmisión, no resultó en una recepción correcta debido a un valor incorrecto en el FCS. El intervalo EIFS debe comenzar seguido de la indicación por parte de la PHY, de que el medio se encuentra ocupado después de la detección del frame erróneo, sin referirse al mecanismo virtual de sensor de portadora. El EIFS se define para proporcionar el tiempo necesario para que otra STA detecte que fue lo que sucedió con la STA donde ocurrió el error, antes de que la primera comience su transmisión. Le recepción de un frame libre de errores durante el EIFS, re-sincroniza la STA al estado actual libre/ocupado del medio, terminando de esta manera el EIFS y el acceso normal al medio (empleando un DIFS y si es necesario, un backoff) continuando posteriormente con la recepción normal de dicho frame.

**Tiempo Backoff Aleatorio**

Una estación que desea iniciar la transferencia de MPDU's de datos y/o de administración, deberá invocar al proceso sensor de portadora para determinar el estado libre/ocupado del medio. Si el medio se encuentra ocupado, la estación deberá postergar su petición hasta que el medio se encuentra libre sin interrupciones por un periodo igual a un DIFS cuando el ultimo frame que se encuentra en el medio se ha recibido correctamente, o bien, cuando se determina

que el medio se encontrará libre sin interrupciones por un periodo igual a un EIFS cuando el ultimo frame en el medio no se haya recibido apropiadamente.
Después del tiempo que el medio permanece libre durante el DIFS o EIFS, la STA genera un periodo de backoff aleatorio para agregar un tiempo de prórroga después de la transmisión, a menos que el contador del backoff contenga un valor distinto de cero, caso en el cual no es necesario llevar a cabo la asignación de un número aleatorio para el tiempo del backoff. Este proceso minimiza las colisiones durante la contención en la que múltiples STA's han aplazado el acceso al medio.

$$\textbf{\textit{Tiempo de Backoff}} = \#\ Aleatorio \cdot Ranura\ de\ tiempo$$

Donde:

- # Aleatorio corresponde a un entero pseudoaleatorio tomado de una distribución uniforme sobre el intervalo $[0,CW]$[19], donde la CW es un entero dentro del rango de valores de las características del medio y
- Ranura de tiempo corresponde al valor característico de la capa PHY.

El parámetro ventana de contención (CW) deberá tomar un valor inicial de *aCWmin*. Cada estación deberá mantener un contador de reintentos cortos (SSRC) así como un contador de reintentos largos (SLRC), ambos tomando un valor inicial de cero. Ambos contadores se incrementan cuando existe un registro de reintento de transmisión de MPDU's largos o cortos.

La CW deberá tomar el siguiente valor en la serie cada vez que un intento de transmisión resulta fallido y por ende, se incrementa el contador de reintento de cada STA, hasta que la CW alcanza el valor máximo aCWmax. Un reintento se define como la secuencia completa de envíos de frames, separados por los SIF's en un intento de entregar un MPDU, tal y como se describe en la sección 9.7 del Estándar.

Una vez que se alcanza éste último valor, el CW continúa con el mismo valor hasta que se reinicia nuevamente. Esto mejora la estabilidad del protocolo de acceso bajo condiciones de alta demanda. Esto se ilustra en la siguiente figura:

[19] Contention Window

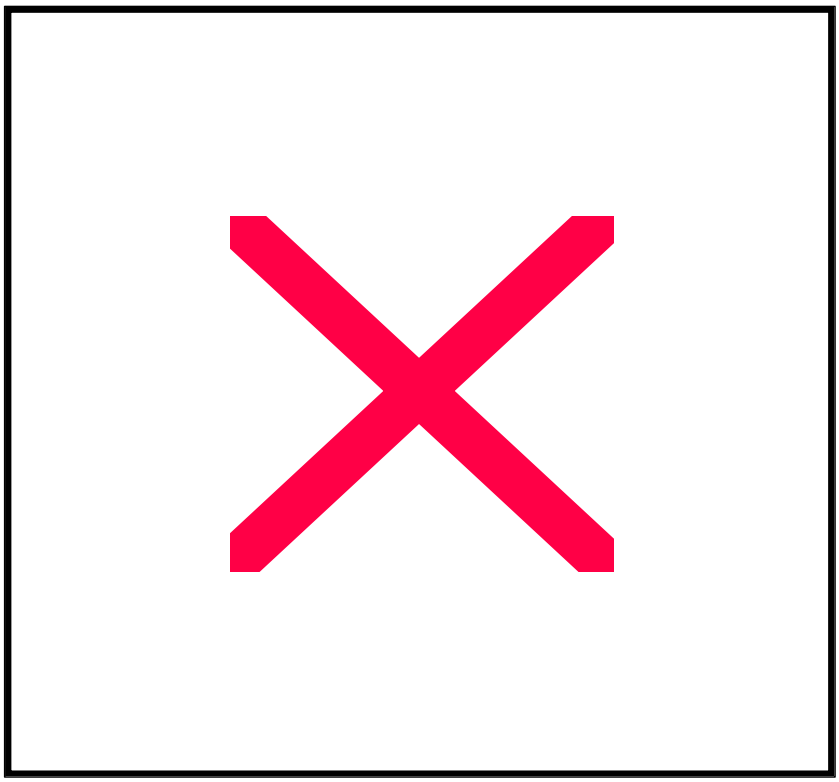


Figura 4.11
*Ejemplo del Crecimiento Exponencial de la CW*

### 4.4.5 Procedimiento de Acceso del DCF

El método de acceso del protocolo CSMA/CA es el fundamento de la DCF. Las reglas de operación varían ligeramente respecto al método de acceso del PCF.

Acceso Básico

El acceso básico se refiere al mecanismo medular que emplea cada STA para determinar si puede transmitir. En general, una STA puede transmitir un MPDU que esté pendiente cuando opera bajo el método de acceso en la DCF, incluso con la ausencia de un PC, o en el CP del método de acceso PCF, cuando el medio determina que se encuentra libre por un periodo mayor o igual a un DIFS, o a un periodo EIFS si en el evento predecesor en el que el medio se encontraba ocupado detectó que el frame fue recibido con un valor de FCS incorrecto. Si bajo estas condiciones se determina que el medio se encuentra ocupado (a través del mecanismo sensor de portadora), y una estación desea iniciar el proceso inicial de envío de frames, entonces se seguirá el proceso de asignación de un backoff que se describe en el siguiente subtema. Existen algunas condiciones donde el backoff

aleatorio será ejecutado inclusive para el primer intento de la secuencia de intercambio de frames.

### Procedimiento de Backoff

Este procedimiento se lleva a cabo cuando las STA's detectan que el medio se encuentra ocupado o bien, que ocurrió una transmisión fallida. Para comenzar con el procedimiento del backoff, la STA asigna un tiempo aleatorio de backoff de acuerdo a la ecuación antes mencionada. Todas las ranuras de backoff ocurren después de un periodo DIFS durante el cual se determina que el medio se encuentra ocupado dentro de la duración de dicho periodo, o enseguida de un periodo EIFS cuando se determinó una transmisión fallida.

Una STA que lleva a cabo el procedimiento de backoff debe emplear el mecanismo sensor de portadora para determinar si es que hay actividad durante cada ranura de backoff. Si no hay actividad en el medio dentro de una duración particular de una ranura, entonces el tiempo asignado al backoff se reducirá.

Si se determina que el medio se encuentra ocupado en cualquier momento de la ranura de backoff, entonces se suspende el procedimiento de backoff; esto es, que el contador del backoff no se decrementará. El medio deberá determinarse como ocupado por un periodo DIFS o EIFS, antes de sea permitida la reanudación del proceso de backoff. Las transmisiones comienzan siempre que el contador del backoff alcanza el valor de cero. Un procedimiento de backoff se lleva a cabo inmediatamente después de que se finaliza cada transmisión, y cuando se cumple que no hay más fragmentos de frames de administración, control o datos, incluso si no existen transmisiones en cola. En el caso de transmisiones sin éxito, el procedimiento de backoff deberá comenzar al final del intervalo del frame ACK recibido.

Si la transmisión se concluyó con éxito, el valor de la ventana de contención se establece en aCWmin antes de que sea asignado el valor aleatorio del backoff, y al mismo tiempo, son actualizados los valores de los contadores de reintentos largos y cortos de cada STA. Esto asegura que cada frame transmitido de una estación siempre se encuentre separado por al menos un intervalo de backoff.

El efecto de este procedimiento es que cuando múltiples STA's han aplazado sus transmisiones y se encuentran dentro del backoff aleatorio, la estación que haya elegido el backoff más pequeño empleando la función aleatoria, entonces será la que gane la contención.

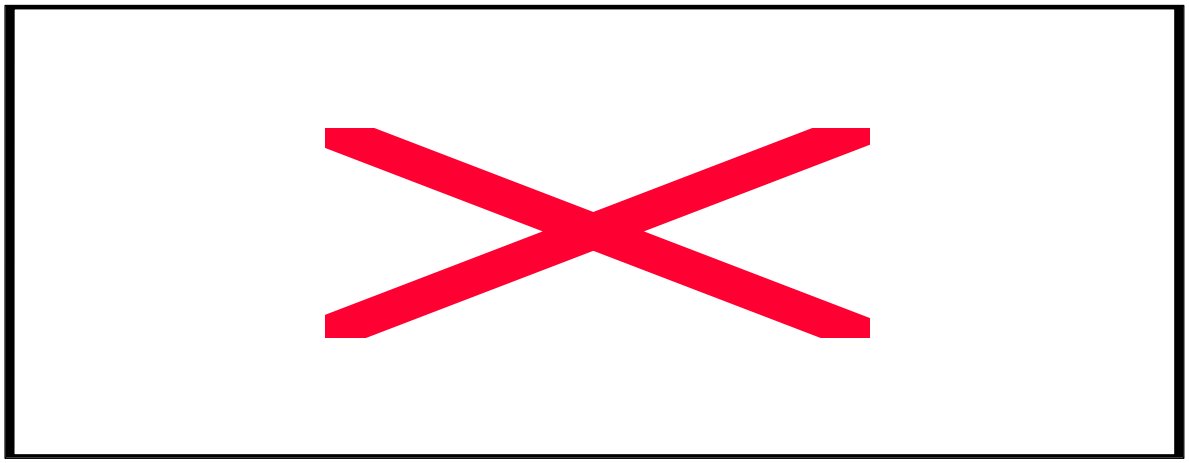


Figura 4.12
*Procedimiento de Contención*
*Entre Diferentes Estaciones*

### 4.4.6 PCF

La PCF (Función de Coordinación Puntual) proporciona la transferencia de datos libre de contenciones. Este mecanismo emplea un protocolo de *encuesta* y respuesta para eliminar la posibilidad de contenciones en el medio. Un coordinador puntual (PC)[20] controla el PCF. El PC siempre se ubica en el AP. Generalmente, el PCF es operado por las estaciones que solicitan que el PC las registre en la lista de "encuesta", y el PC regularmente también "encuesta" a las estaciones mientras entrega el tráfico habitual a las estaciones restantes. El PCF está constituido dentro del DCF y ambos operan de manera simultánea. El PCF emplea el intervalo PIFS en lugar del DIFS. El PC comienza con un periodo de operación llamado periodo de contención libre (CFP), durante el cual, el PCF se encuentra operando. Este periodo se llama de contención libre porque el acceso al medio es completamente controlado por el PC, y el DCF es prevenido de ganar el acceso al medio. El CFP aparece de manera periódica para proporcionar un servicio *iso-síncrono* a las estaciones asociadas. El CFP también alterna con los periodos de contención donde operan las reglas convencionales del DCF y todas las estaciones pueden competir por el acceso al medio. El Estándar requiere que el periodo de contención sea lo suficientemente largo como para contener la menor longitud de un frame así como su verificación.

El CFP comienza cuando el PC gana el acceso al medio, empleando los procedimientos habituales del DCF, y posteriormente envía un frame tipo Beacon. Este tipo de frames reuqieren que se transmitan de manera periódica para que el PC pueda competir por el medio. El tráfico en el CFP consistirá en los frames enviados desde el PC hata una o más estaciones, seguido de la confirmación de

[20] Point Coordinator

dichas estaciones. Además, el PC envía un frame "encuesta" libre de contención (CF-Poll)[21] para aquellas estaciones que han solicitado el servicio libre de contención. Si la estación tiene datos que enviar entonces la respuesta es el CF-Poll. Para un empleo eficiente del medio, es posible adjuntar los frames de confirmación y el CF-Poll dentro de los frames de datos.

Durante el tiempo del CFP, el PC se asegura que el intervalo ente los frames que emplean el medio, no sean más largos que el PIFS. Esto con la intención de prevenir que una estación se encuentre en operación mientras el DCF intenta ganar acceso al medio. Hasta que transcurre el intervalo CFP, el PC envía un SIFS y espera la respuesta; en caso contrario lo intenta nuevamente. El NAV previene a las estaciones de acceder al medio durante la transmisión de un CFP. El uso de los PIFS está dirigido para aquellas estaciones que no reciban el frame beacon. El PC anuncia el final del CFP transmitiendo un frame de fin libre de contención (CF-End)[22]. Éste reinicia el NAV y las estaciones comenzarán la operación del DCF de manera independiente.

Existen problemas con el PC que encabezan las actividades en curso para que el protocolo funcione adecuadamente. Entre muchos otros, se incluyen los retrasos impredecibles de los frames beacon y las duraciones desconocidas de las transmisiones que realizan las estaciones "encuestadas". En un TBTT[23] (Tiempo de Transmisión del frame Beacon Objetivo), el PC agenda al frame bacon como el próximo frame a transmitir; dicho frame podrá ser transmitido cuando se determine que el medio se encuentra inactivo por lo menos en un periodo PIFS.

### 4.4.7 Funciones Adicionales de la Capa MAC

Autenticación

La autenticación es un mecanismo que proporciona la identificación de una estación con otra dentro de la WLAN. Sin embargo, es más común que sea empleada cuando una estación pertenece a una red tipo infraestructura para prevenir a los usuarios no autorizados. El siguiente capítulo aborda a detalle esta situación.

Asociación

La asociación es el mecanismo a través del cual el Estándar 802.11 proporciona transparencia a la movilidad entre estaciones. La asociación sólo puede ocurrir cuando el proceso de autenticación ha sido completado.

[21] Contention-Free Poll
[22] Contention-Free End
[23] Target Beacon Transmission Time

Cuando una estación móvil envía una envía una petición para conectarse a una WLAN, envía una petición de asociación al AP. Dicha petición incluye información de las capacidades de la estación, tales como la tasa de transmisión que soporta la estación, las capacidades libres de contención, las opciones de autenticación y la solicitud de servicios libres de contención. Adicionalmente, se incluye información acerca del tiempo de latencia en el que se encuentra la estación, si es que opera en el modo de ahorro de energía.

Cuando un AP responde a una estación una petición de asociación, dicha respuesta incluye una indicación del status del AP; este status es el indicativo de la asociación exitosa o fallida. Si la petición es rechazada, la razón se encuentra incluida en el status.

Cuando una estación móvil pierde contacto con un AP, dicha estación deberá comenzar una nueva asociación; debido a que el DS (sistema de distribución) debe contener toda la información acerca de de la ubicación de cada estación móvil, la estación que deja de tener comunicación con un AP ejecuta el proceso llamado re-asociación en el que solicita nuevamente el contacto con un nuevo AP.

### Filtro de Direcciones

Es altamente probable que más de una WLAN se encuentre operando dentro de la misma área y/o canal. En este caso el receptor debe examinar más de una dirección destino para efecto de recibir los frames correctos. El Estándar 802.11 incorpora tres direcciones en cada frame de datos y administración que pueden ser recibidos por la estación. Adicionalmente a la dirección destino, estos frames también incluyen un identificador del BSS al que pertenecen. Una estación debe emplear ambos tipos de direcciones MAC (el BSSID y la dirección MAC) cuando se trata de tomar decisiones en la recepción, de acuerdo al estándar.

### Administración de potencia

La administración de potencia es un proceso completamente distribuido y administrado por las estaciones móviles. Tal administración comprende dos partes: las funciones de la estación cuando opera en modo de baja potencia y las funciones de las estaciones que desean comunicarse con esa estación.

Una estación que entra en el modo de operación de baja potencia (es el estado donde se ha apagado el receptor y transmisor para conservar la energía), debe completar una rutina de intercambio de datos con otra estación indicándole a ésta última el tipo de administración de energía que tiene en ese momento. Esta información está contenida en el encabezado del frame. El Estándar no especifica

cuándo una estación debe entrar o dejar el estado de latencia, sólo indica cómo la transición toma lugar.

La estación debe permanecer *despierta* por un cierto periodo de tiempo, llamado Ventana de Mensaje Indicadora del Tráfico Ad Hoc (ATIM)[24]. El momento más próximo en el que una estación puede volver a entrar en el modo de latencia es en la conclusión de la ventana ATIM. La razón de por qué una estación debe esperar este intervalo de tiempo antes de la latencia es que probablemente otras estaciones estarán intentando enviar frames durante el ATIM. Si la estación que se que quiere estar en latencia recibe el frame ATIM, deberá confirmar la recepción de dicho frame y esperar hasta el final de la próxima ATIM seguido del Bacon, de manera que permita a las demás estaciones completar sus secuencias de intercambio de frames.

Una estación que desea transmitir a otra, debe estimar en primer lugar el estado en que se encuentra. Si la estación transmisora determina que la estación receptora se encuentra en latencia, entonces la estación origen retrasa su transmisión hasta que recibe la confirmación del frame ATIM.

Sincronización

La sincronización es el proceso que llevan a cabo las estaciones que pertenecen a cierta BSS para que las comunicaciones puedan efectuarse al mismo nivel. La capa MAC proporciona el mecanismo de sincronización que permite soportar diferentes capas PHY que emplean saltos en frecuencia o mecanismos basados en tiempo donde los parámetros de la PHY varían con el tiempo.

El proceso involucra a los frames bacon, para anunciar la presencia del BSS. Una vez que es encontrada una BSS, la estación se asocial con la BSS y establece una base de tiempo en común, proporcionado por una función de sincronización temporal (TSF[25]). La función de sincronización es muy simple: una estación actualizará su temporizador TSF con el valor que recibe del frame bacon emitido por el AP, modificado por cualquier proceso temporal que requiera la optimización del medio.

La estación móvil que recién se asocie a una BSS comenzará con un valor inicial de cero y posteriormente enviará un frame bacon. La estación receptora enviará un frame beacon que contiene un tiempo aleatorio.

[24] Ad Hoc Traffic Indication Message
[25] Timer Synchronization Function

CAPÍTULO CINCO

# Seguridad en las WLAN's

## 5.1 Introducción

Actualmente las redes WLAN se han convertido en una aplicación importante dentro de las organizaciones que requieren una alternativa para incrementar el desempeño de su red de datos. El principal reto de los administradores de la red es el de integrar las WLAN a las redes cableadas tradicionales, incluyendo todas las características de éstas, como son: seguridad, administración y escalabilidad. De éstas, la seguridad se considera de extrema importancia. El control de acceso asegura que el intercambio de datos se realice sólo entre usuarios autorizados. La privacidad asegura que los datos transmitidos puedan ser recibidos e interpretados sólo para los usuarios a los que va dirigida dicha información.

El acceso a una red cableada está controlado por el acceso a un puerto físico ethernet. Por tanto, el control de acceso a una red LAN puede verse en términos de un acceso físico a los puertos de la LAN y por ende la privacidad no puede verse comprometida a menos de que alguien pueda emplear equipo especializado para interceptar las transmisiones que se encuentren en proceso.

En una WLAN, los datos transmitidos se propagan a través del aire mediante ondas de radio, así que ésta señal puede ser recibida por cualquier cliente WLAN que se encuentre dentro del área de servicio proporcionada por el transmisor. Dado que las ondas de radio pueden pasar a través de techos, pisos y paredes, los datos transmitidos pueden alcanzar a usuarios mal intencionados de diferentes pisos o incluso fuera de los edificios donde se localizan los transmisores. La instalación de una WLAN puede visualizarse como la instalación de puertos Ethernet en cualquier lado, incluyendo espacios abiertos. El Estándar 802.11 incluye algunos componentes para asegurar el control de acceso y privacidad, pero dichos componentes deberán implementarse en cada uno de los dispositivos de una WLAN. Una organización con cientos de usuarios WLAN necesitará una solución sólida en materia de seguridad que pueda ser administrada de manera central en un punto de control.

## 5.2 Servicios de Autenticación del Estándar 802.11

Como se mencionó en el primer capítulo, para que exista el intercambio de datos entre dos elementos de una WLAN, se debe asegurar que ambos dispositivos pertenezcan a la misma IBSS y posteriormente, que dichos equipos se encuentren asociados. De forma esquemática, esto se representa en el siguiente diagrama de estado:

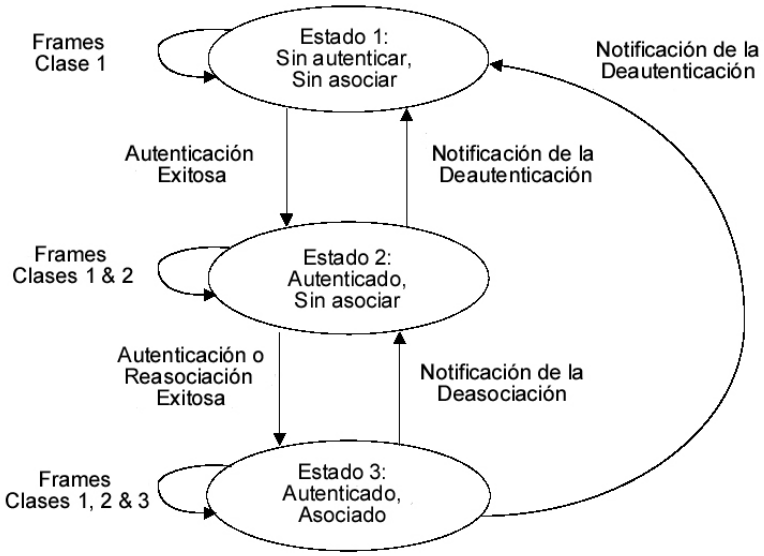



Figura 5.1
*Diagrama de Estado*
*de la Autenticación y asociación*
*en el Estándar 802.11*

El estado actual que existe entre dos estaciones (la transmisora y la receptora) determina los tipos de frame que pueden ser intercambiados por el par de STA's. El estado de la STA transmisora dado por la figura anterior se encuentra referido a la STA que intenta recibir. Los tipos de frame permitidos se agrupan dentro de tres clases y dichas clases corresponden al estado de la estación. En el Estado 1, sólo se permiten frames de Clase 1. En el Estado 2, se permiten los tipos de frame 1 y 2. En el Estado 3, se permiten las tres clases de frame: Clase 1, Clase 2 y Clase 3. Las Clases de frame son las siguientes:

**a) Frames Clase 1**

Frames de Control

RTS, CTS, ACK, CF-End+ACK,

Frames de Administración

Pruebas de petición-respuesta, Beacon, Autenticación (una autenticación exitosa permite que la estación intercambie frames Clase 2; de lo contrario la STA permanece en el Estado 1), Deautenticación (la notificación de autenticación ocurre cuando el Estado 2 o el Estado 3 cambian al Estado 1), Mensaje de anuncio indicador de tráfico (ATIM).

Frames de Datos:

Frames de datos con los bits FC "DS origen" y "DS Destino" con un valor de cero.

**b) Frames Clase 2 (sólo si se ha completado la autenticación)**

b.1) Frames de Administración

- Petición/respuesta de asociación: la asociación exitosa permite el intercambio de frames Clase 3, la asociación no exitosa deja a la STA en el Estado 2.
- Petición/respuesta de reasociación: la reasociación exitosa permite el intercambio de frames Clase 3. Una petición de reasociación no exitosa deja a la STA en el Estado 2 (con respecto a la STA que envió el mensaje de reasociación). Los frames de reasociación sólo deberán ser enviados si la STA emisora se encuentra asociada en el mismo ESS.
- Deasociación: se presenta cuando el Estado 3 cambia al Estado 2 de la Estación. Dicha estación deberá asociarse nuevamente si desea emplear el DS.

**c) Frames Clase 3 (sólo si se ha completado la asociación; permitidos sólo dentro del Estado 3)**

- Frames de Datos
- Frames de Administración: Deautenticación
- Frames de Control: PS-Poll

El Estándar 802.11 define dos subtipos de servicios de autenticación: Sistema Abierto (OS[1]) y Llave compartida (SK[2]). El subtipo de servicio que se está empleando se encuentra definido en los frames de administración. Así que los frames de autenticación se diferencian por sí mismos de un algoritmo de autenticación. Todos los frames de de un subtipo de Autenticación deberán ser frames unicast como parte de la autenticación llevada a cabo por un par de estaciones (por ejemplo, la autenticación en grupo o *multicast* no es permitida).

[1] Open System
[2] Shared Key

Estos tipos de autenticación constituyen un tipo de seguridad que será descrito a continuación.

## 5.3 Seguridad de Básica en WLAN's

La seguridad básica en las WLAN's comprende el empleo de los siguientes mecanismos:

- SSID[3] (Identificador del Conjunto de Servicio)
- WEP[4] (Privacidad Equivalente LAN)
- Autenticación con Sistema Abierto (OS) o Llave Compartida (SK)

La combinación de estos sistemas ofrece un control de acceso y privacidad rudimentarios, dado que su estructura misma es muy vulnerable.

### 5.3.1 Identificador del Conjunto de Servicio (SSID)

Una característica empleada en las WLAN's es el manejo de un nombre, el SSID, que proporciona un nivel de seguridad rudimentario. El SSID es análogo a un nombre de red común para las estaciones y los AP's dentro de un subsistema WLAN.

El SSID es una pieza de información que puede ser anunciado o pre-configurado manualmente en la estación. El SSID puede ser solicitado por un frame de prueba-respuesta cuando un cliente intenta integrarse a un subsistema WLAN o puede ser detectado como parte de una serie de frames *bacon* enviados por un AP. Sin embargo, un AP envía los SSID's en los frames *bacon* de manera "automática"; incluso si esta opción es deshabilitada, un intruso o *hacker* puede detectar los SSID's a través de lo que se conoce como s*niffing*, que consiste en un monitoreo externo de la red.

### 5.3.2 Privacidad Equivalente LAN (WEP)

La encriptación WEP *mezcla* la comunicación entre el punto de acceso y los dispositivos cliente para mantener la privacidad de la comunicación. El AP y el cliente emplean la misma llave WEP para encriptar y desencriptar las señales de radio.

El algoritmo WEP puede visualizarse como un libro electrónico de códigos en el cual un bloque de texto plano (información sin codificar) es sometido a una función

[3] Service Set Identifier
[4] Wired Equivalent Privacy

XOR con una secuencia pseudo-aleatoria de la misma longitud. Dicha secuencia es generada por el algoritmo WEP.

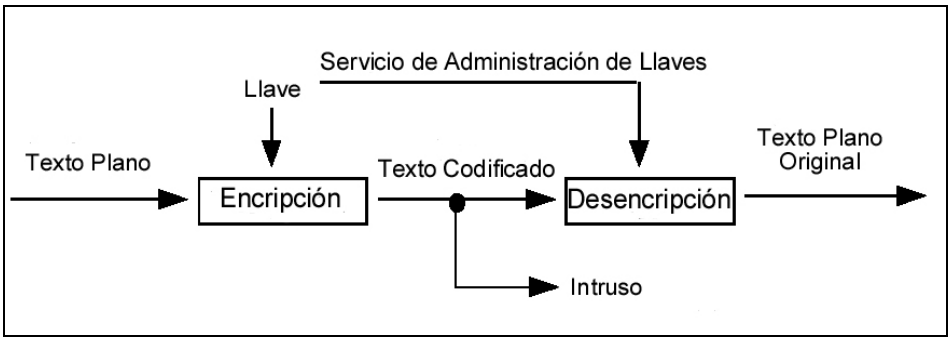



Figura 5.2
*Diagrama de Bloques*
*del Mecanismo WEP*

Refiriéndonos a la figura anterior y observando de derecha a izquierda, el cifrado comienza con una *llave secreta* que es distribuida hacia todas las STA's por un servicio de administración de llaves externo. El protocolo WEP es un algoritmo simétrico que emplea la misma llave para el cifrado y descifrado.

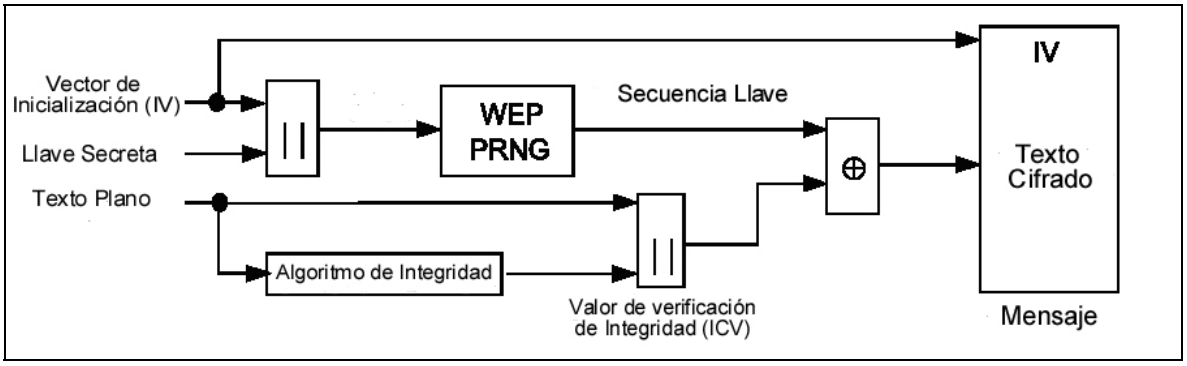



Figura 5.3
*Proceso de Encriptación WEP*

La llave secreta es concatenada con un *vector de inicialización* (IV) y el resultado es introducido en el generador de números pseudo-aleatorio (PRGN[5]). El PRNG entrega una secuencia llave de octetos pseudo-aleatorios de la misma longitud que el número de octetos de datos que están siendo transmitidos, además de 4 octetos adicionales (debido a que la secuencia llave es empleada para proteger el *valor de verificación de integridad* ICV[6], así como los datos).

[5] Pseudo-Random Number Generator
[6] Integrity Check Value

Al texto plano de los MPDU's se les aplica dos procesos. Para proteger contra la modificación no autorizada de datos, un algoritmo de integridad opera sobre el texto plano para producir el ICV. La salida del proceso es un *mensaje* que contiene el IV y un texto cifrado.

El PRNG WEP es el componente crítico de este proceso, debido a que transforma una llave secreta relativamente corta en una secuencia llave arbitrariamente larga. Esto simplifica en gran medida la tarea de distribución de llaves, ya que sólo se maneja una llave secreta que emplean las dos estaciones para comunicarse. El IV extiende la vida útil de la llave secreta y proporciona la auto-sincronía propia del algoritmo. La llave secreta se mantiene constante, mientras que el IV cambia periódicamente. Cada cambio en el IV se traduce en una nueva secuencia llave, por lo que existe una correspondencia de uno a uno entre el IV y la secuencia llave.

El IV puede cambiar tan frecuentemente como MPDU's existan por transmitir, dado que el vector viaja junto con el mensaje y el receptor siempre será capaz de descifrar cualquier mensaje. El IV es transmitido libremente debido a que no es posible que proporcione información alguna acerca de la llave secreta a un probable intruso y a que su valor debe ser conocido por la estación receptora de manera que pueda llevar a cabo la desencriptación.

El algoritmo WEP es aplicado al cuerpo del frame de un MPDU. La tercia que forman los octetos IV, Cuerpo del Frame y el ICV conforman el conjunto de datos que son enviados en cada frame. Para los frames protegidos con el WEP, el primero de los cuatro octetos del cuerpo del frame contiene el campo IV del MPDU. El IV es seguido por el MPDU, que tiene como consecuente al ICV. El algoritmo de Verificación de Integridad del WEP es el CRC-32, como se definió en el capítulo 3.

Refiriéndonos a la siguiente figura y observando de derecha a izquierda, el desciframiento comienza con la llegada del mensaje. El IV del mensaje entrante deberá ser empleado para generar la secuencia llave necesaria para descifrar el mensaje. Combinando el texto cifrado con la adecuada secuencia llave se obtiene el texto plano original y el ICV. El correcto descifrado deberá ser verificado a través algoritmo de verificación de integridad y llevado a cabo sobre el texto plano recuperado, comparando la salida del ICV' y el ICV transmitidos junto con el mensaje. Si el ICV' no es igual al ICV, el MPDU recibido es considerado como erróneo y es enviada una indicación de error a la administración MAC. Los MSDU's con MPDU's erróneos (debido a la imposibilidad de descifrar) no serán transmitidos a la LLC.

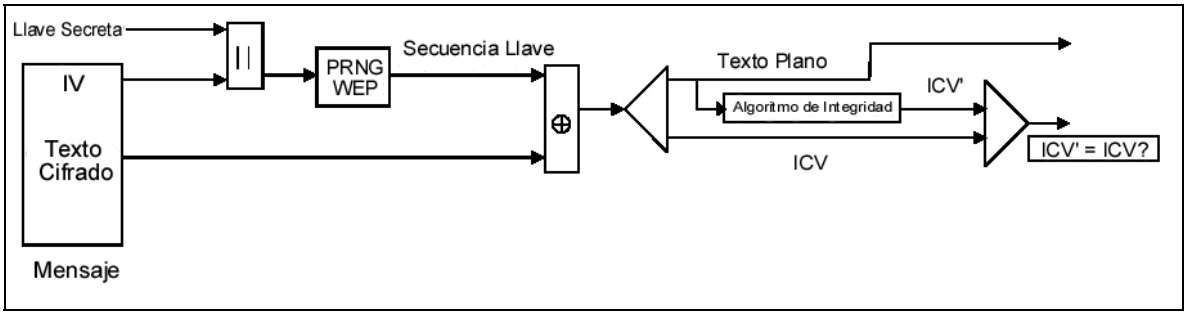



Figura 5.4
*Proceso de Desencriptación WEP*

## Expansión del Cuerpo del Frame WEP

La siguiente figura muestra el cuerpo de un frame que ha sido construido por el algoritmo WEP.

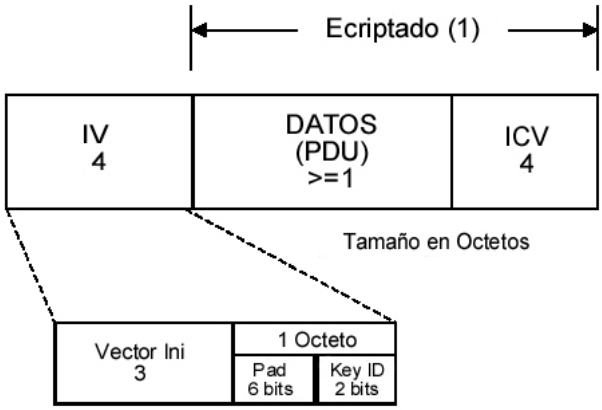



Figura 5.5
*Cuerpo del Frame Construido por el WEP*

El ICV WEP debe ser un campo de 32-bits que contiene el código CRC-32, como se definió en el capítulo 3, calculado sobre el PDU de datos, y también en la figura anterior. El Cuerpo del Frame expandido deberá incluir un campo IV de 32 bits precedido inmediatamente por el Cuerpo del Frame original. Dicho campo, deberá contener tres subcampos: un campo de tres octetos que contiene el vector de inicialización, un campo de 2 bits que contiene el identificador de llave (ID KEY) y un campo de 6 bits llamado *Pad*. El identificador de llave contiene uno de cuatro posibles valores que de la llave secreta para desencriptar el Cuerpo del Frame. El contenido del campo *Pad* deberá ser cero.

### 5.3.3 Autenticación en Sistema Abierto

Esencialmente es un algoritmo de autenticación nulo. Cualquier STA que solicite la autenticación con este algoritmo puede llegar a autenticarse si la opción dot11Autentication Type en la estación receptora se encuentra habilitada la opción de Autenticación por Sistema Abierto.

Este sistema de autenticación involucra una secuencia de transacción de dos pasos. El primer paso en la secuencia es la verificación de la identidad y la solicitud de autenticación. El segundo paso de la secuencia es el resultado de la autenticación. Si el resultado es satisfactorio, las STA's estarán mutuamente autenticadas. Gráficamente se muestra a continuación.

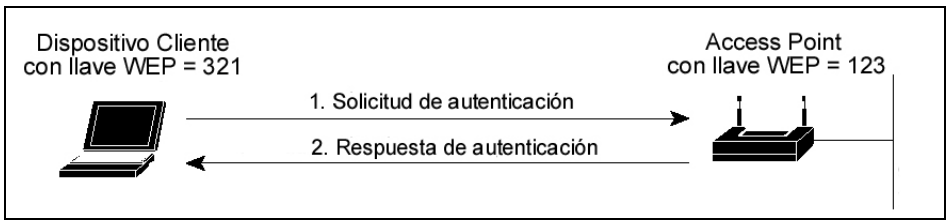



Figura 5.6
*Autenticación en Sistema Abierto*

### 5.3.4 Autenticación con Llave Compartida (SK)

La autenticación con llave compartida soporta la autenticación de aquellas estaciones que contengan una llave compartida y de aquellas que no la tengan. Este mecanismo se lleva a cabo sin la necesidad de transmitir la llave secreta en el medio; sin embargo, requiere que sea empleado el mecanismo WEP. Por ende, este mecanismo sólo se encontrará disponible si se encuentra implementada la opción WEP.

La llave secreta es entregada a las STA's participantes mediante un canal seguro que es independiente del Estándar 802.11. Durante el intercambio de frames de autenticación, se transmiten los códigos encriptados. Esto facilita el descubrimiento no autorizado del número de la secuencia pseudo-aleatoria (PRN) para la llave/IV empleada para el intercambio. En las implementaciones se debe evitar el empleo de la misma llave/IV para los frames subsecuentes.

El mecanismo funciona de la siguiente forma:

1. La estación solicitante envía un frame de solicitud de autenticación al AP.
2. El AP envía como respuesta una cadena de datos sin encriptar hacia el dispositivo solicitante.

3. El dispositivo recibe esta cadena y la encripta, enviándola nuevamente al AP.
4. Si la cadena fue encriptada correctamente, el AP permite la autenticación del dispositivo solicitante.

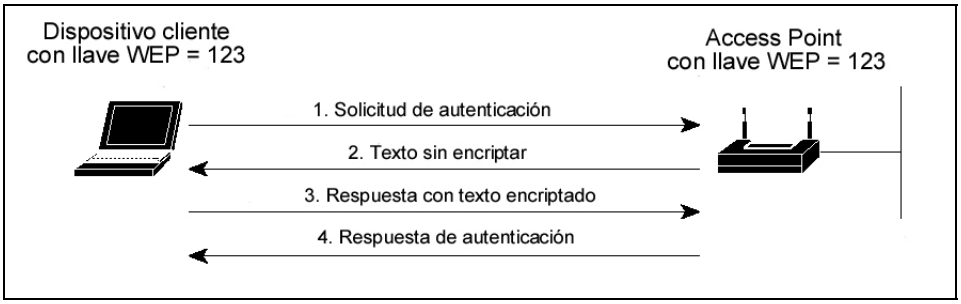



Figura 5.7
*Autenticación en Sistema Abierto*

La deficiencia de este sistema radica en que el texto sin encriptar y el texto encriptado pueden ser monitoreados, con lo cual deja al AP expuesto a los ataques de un intruso que pueda calcular las llaves WEP por medio de la comparación de las cadenas sin encriptar y las encriptadas. Debido a esta debilidad, este tipo de autenticación puede considerarse menos segura que el mecanismo de sistema abierto. Ambos sistemas, no depende de un servidor RADIUS. En la siguiente sección se describe el uso de este componente.

## 5.4 Seguridad de Nueva Generación

Las políticas de seguridad son únicas en cada organización. Para la mayoría de las redes, el empleo de llaves WEP estáticas no resulta ser suficiente ya que son introducidas manualmente en los AP's y los clientes. Aunque el mecanismo WEP emplea una cadena RC4 simétrica para lograr la encriptación, las llaves estáticas son relativamente fáciles de descifrar.

En base a lo expuesto con anterioridad en el subtema anterior, existen tres componentes principales para implementar un sistema de seguridad en una red WLAN:

- Un algoritmo de autenticación
- Un esquema de encriptación de datos para mantener la privacidad de los datos y,
- Una estructura que administre la autenticación entre el cliente, el punto de acceso y un servidor para el Servicio de Autenticación Remoto de Usuarios Dial-In (RADIUS[7])

[7] Remote Authentication Dial-In User Service

Los administradores de Red tienen la opción de implementar éstas funciones en la capa 2 (donde se aplica el Estándar 802.11), u optar por el empleo de una VPN IPsec en la capa 3.

Los algoritmos seleccionados para la seguridad de cada componente y la manera en son implementados determinan que tan resistente es el ambiente WLAN a los ataques. Por ejemplo, el siguiente diagrama de la empresa CISCO nos muestra esta idea.

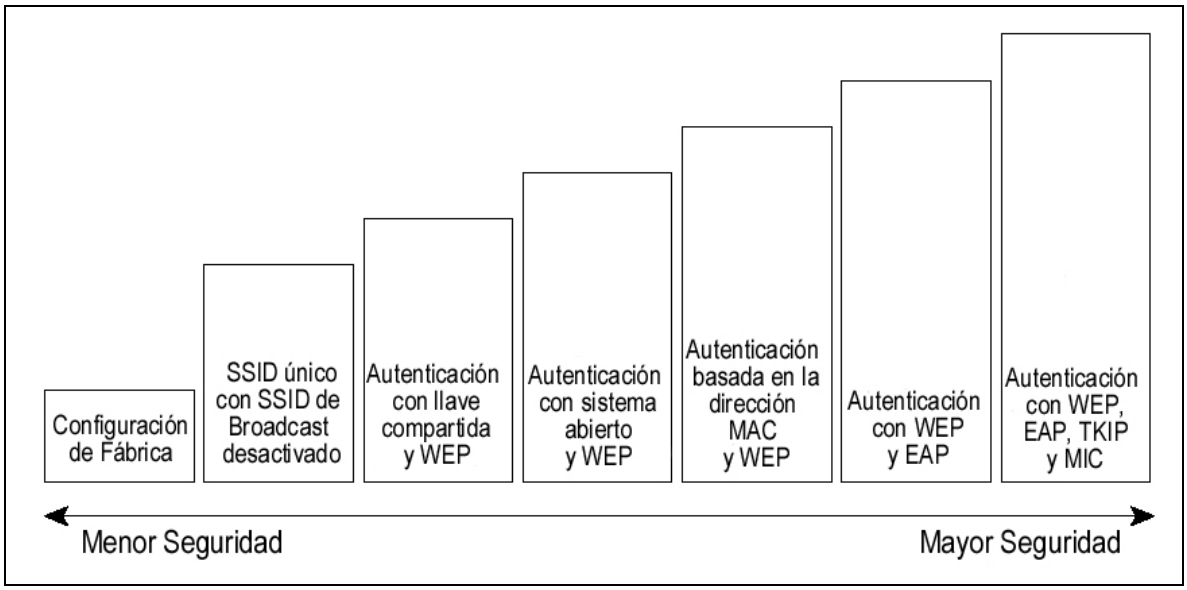



Figura 5.8
*Robustez de la Seguridad*
*En las WLAN*

Como una guía de implementación de una WLAN segura, el fabricante CISCO nos recomienda lo siguiente:

- ***Autenticación basada en el usuario,*** en lugar de utilizar la autenticación basada en un dispositivo, de manera que un intruso no pueda tener acceso a la red mediante el robo de la identificación de un equipo o su simulación.
- ***Administración centralizada***, para que las credenciales de identificación puedan ser almacenadas en un equipo específico y evitar ser distribuidas en cada AP.
- ***Sesión dinámica basada en ecriptación de llaves***, que deberán ser cambiadas automáticamente durante ciertos intervalos de tiempo y cuando ocurran las re-autenticaciones, haciendo más difícil la tarea descubrir las llaves secretas.
- ***Autenticación mutua,*** de manera que los usuarios no se asocien a un AP no autorizado. La autenticación mutua, adicionalmente a la validación de

credenciales de un cliente que intenta acceder a los recursos de la red, verifica que el AP es válido y autorizado para proporcionar dicho acceso. Debido a que los AP son pequeños y de bajo costo, es posible que un visitante o intruso, incluyendo a los mismos empleados, podrían instalar un AP no autorizado, exponiendo a la organización a los ataques por denegación de servicios (DoS[8]).

Adicionalmente a la selección de tecnologías para llevar a cabo la autenticación, autorización y encriptación de datos, las organizaciones deberán llevar a cabo políticas dentro de sus redes que determinen los derechos de acceso que se le asignan a cada usuario y que deberán indicar las acciones a realizar una vez que una conexión ya no sea asociada a un puerto físico especifico. Aquí es donde el esquema ofrecido por IPsec dentro de una VLAN entra en juego, porque las redes dentro de la capa 3 son capaces de diferenciar a los usuarios por su encabezado IP. Debido a que la seguridad de las WLAN opera en la capa 2, la identificación se limita al dispositivo (no al usuario), si es que se opta por un esquema de seguridad basada en la dirección MAC de la Tarjeta de Interfase Red (NIC).

Para incrementar la seguridad del Estándar 802.11, se ha desarrollado un nuevo Estándar llamado 802.11i. Adicionalmente al *establecimiento y administración de llaves*, también define mejoras en cuanto la *encriptación y autenticación.* Dicho estándar también incorpora adiciones en la autenticación del estándar 802.1x. El Estándar IEEE 802.1x está siendo implementado en muchos de los estándares de la serie 802 con el uso de un servidor de autenticación RADIUS. Este tipo de servidores, proporcionan los servicios de Autenticación, Autorización y manejo de cuentas, y a pesar de que mejora la seguridad de las WLAN, no resuelve todos los problemas en esta materia. Por ello se recurre a esté método como un complemento para robustecer los mecanismos de seguridad.

### 5.4.1 El Estándar IEEE 802.1X

El Estándar IEEE 802.1X define un mecanismo para el control de acceso a la red basado en puertos para proporcionar la autenticación y autorización de los dispositivos que se encuentren conectados a diferentes LAN bajo el Estándar 802. También es empleado para distribuir las llaves secretas de las WLAN's habilitando la autenticación y autorización de llaves públicas entre los AP's y los Nodos Móviles (MN's[9]). En este estándar, *los puertos* representan la asociación entre los AP y los MN.

Existen tres componentes principales en el estándar: *el solicitante, el Autenticador y el Servidor de Autenticación.* El solicitante regularmente es un MN que requiere un

[8] Denial of Service
[9] Mobile Nodes

acceso a la WLAN. El autenticador representa al Servidor de Acceso a la Red y normalmente es un AP. Por último, un servidor RADIUS es comúnmente usado como el servidor de autenticación, aunque pueden emplearse servidores compatibles. En el Estándar IEEE 802.11, dicho servidor puede estar físicamente integrado dentro del AP.

Como se muestra en la figura 5.9, tanto el solicitante como el autenticador contienen un PAE[10] (Entidad de Acceso al Puerto) que opera los algoritmos y protocolos asociados con los mecanismos de autenticación. El autenticador PAE controla el estado autorizado/no autorizado de su *Puerto Controlado* dependiendo de la salida del proceso de autenticación. Antes de que el solicitante sea autenticado, el autenticador emplea el *Puerto no Controlado* para comunicarse con el PAE del solicitante. El autenticador bloqueará todo el tráfico, exceptuando el de los mensajes del tipo 802.1X. Dicho estándar emplea el Protocolo Ampliado de Autenticación (EAP[11]) para proporcionar otros esquemas de autenticación, como son el MD5[12], TLS[13], TTLS[14] y PEAP, entre otros. El Estándar 802.11x también define el protocolo *EAP sobre LAN's* (EAPOL)[15] que encapsula los mensajes EAP entre el solicitante y el PAE autenticador.

Para efecto de que el servidor RADIUS pueda autenticar a los usuarios mediante el uso del EAP, el PAE autenticador encapsula los mensajes EAP con el mismo formato que el RADIUS y los envía a éste, asumiendo que el RADIUS es el servidor de autenticación. Una vez que el solicitante es autenticado exitosamente, el *Puerto Controlado* del autenticador es autorizado. Los paquetes provenientes del solicitante viajarán ahora a través del *Puerto Controlado* y de ahí a los servicios de red que sean solicitados.

[10] Port Access Entity
[11] Extensible Authentication Protocol
[12] Message Digest 5
[13] Transport Layer Security
[14] Tunneled TLS
[15] EAP over LAN's

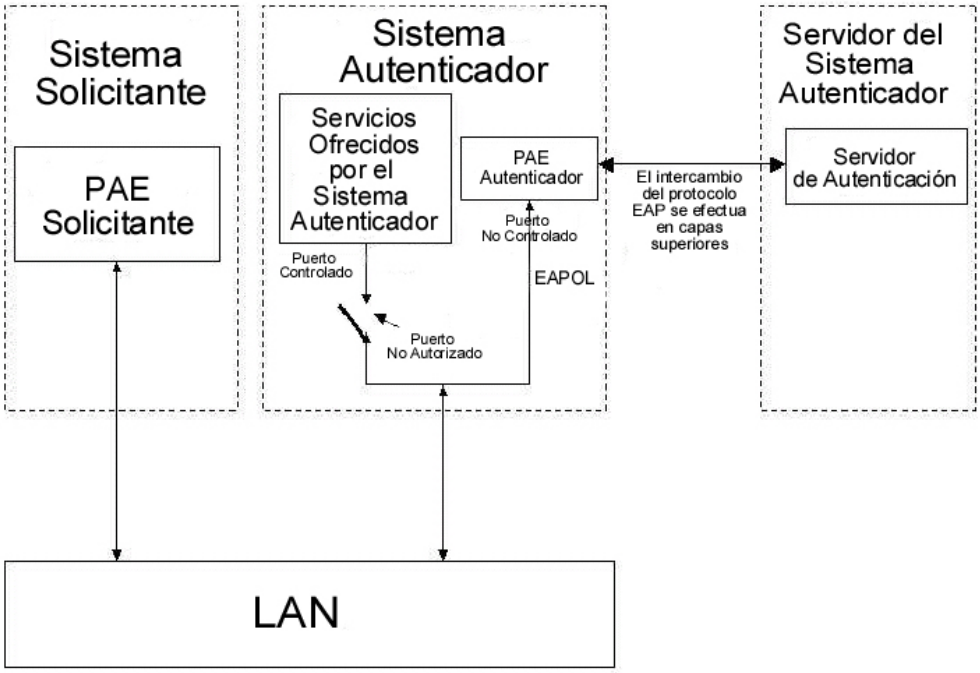



Figura 5.9
*Esquema del Estándar 802.1x*

### 5.4.2 Protocolo Extendido de Autenticación (EAP)

El Estándar 802.1X emplea el protocolo EAP para permitir una amplia variedad de mecanismos de autenticación. La siguiente figura muestra la interacción de este mecanismo con otras capas.

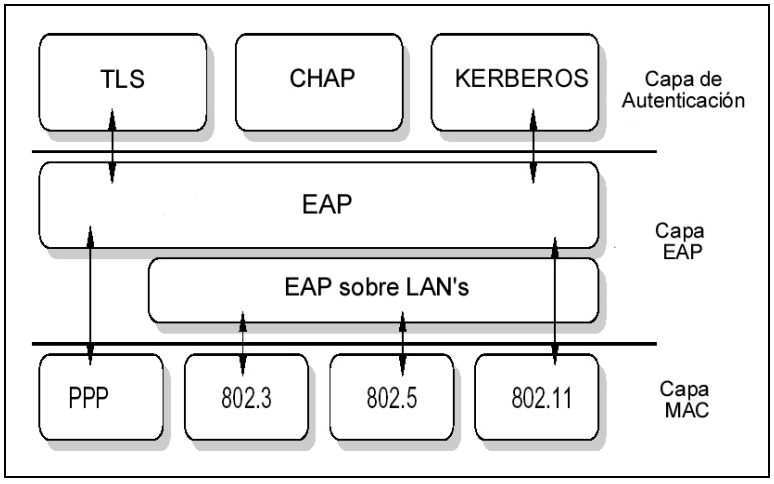



Figura 5.10
*Interacción del EAP con otras Subcapas*

En el protocolo EAP existen cuatro tipos de mensajes: solicitud, respuesta, éxito y negación. La siguiente figura muestra una sesión de autenticación típica.

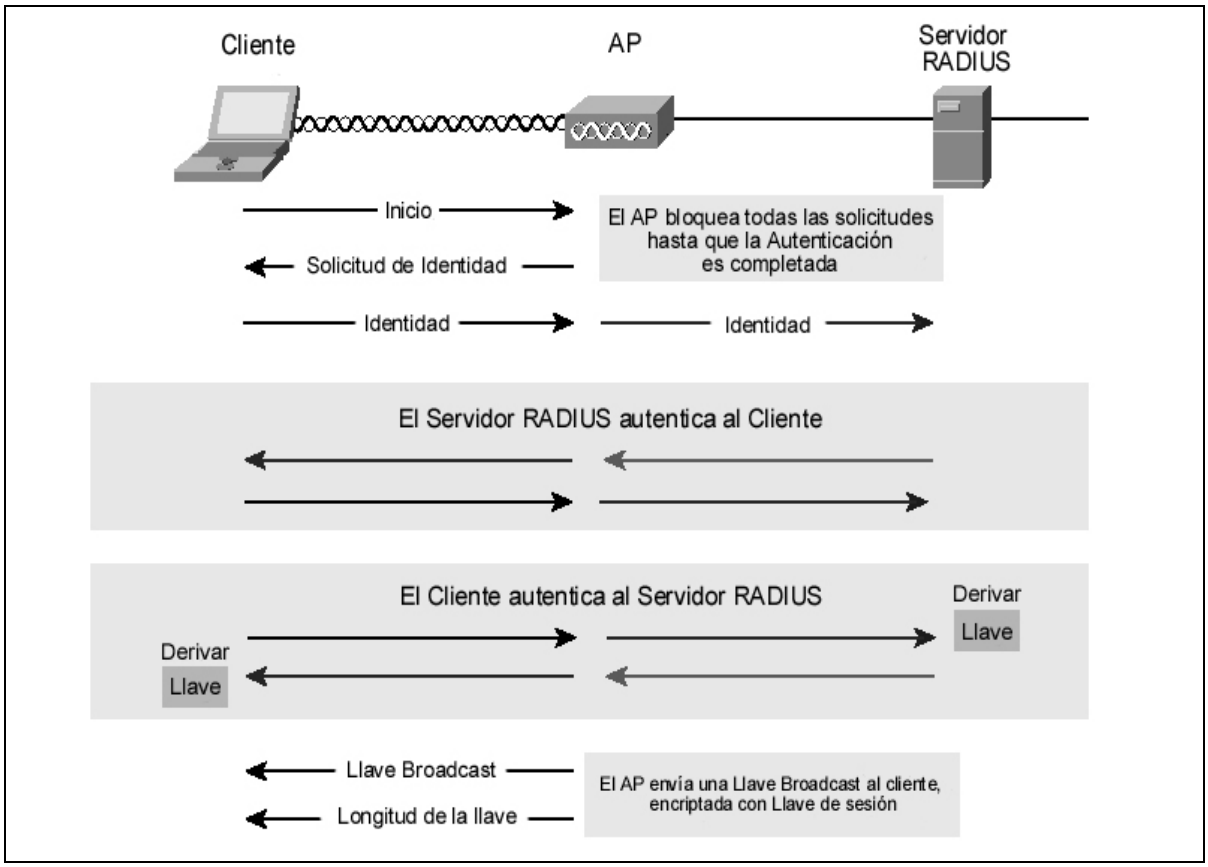



Figura 5.11
*Sesión de Autenticación EAP*

El protocolo es *extendido* porque permite que cualquier mecanismo de autenticación pueda ser encapsulado dentro de los mensajes *solicitud/respuesta*. El protocolo adquiere flexibilidad al operar en la capa de Red en lugar de la capa de Enlace. Debido a esto, el EAP puede direccionar los mensajes a un servidor centralizado en lugar de un puerto de red para la toma de decisiones.

El AP debe permitir el tráfico EAP antes de que suceda la autenticación. Para que esto pueda tener efecto, es empleado un modelo de puertos dual, que se mencionó en la sección pasada. Los mensajes EAP son encapsulados por si mismos. El protocolo EAP sobre LAN's (EAPOL) transporta los paquetes entre el autenticador y el solicitante. Un mensaje *llave EAPOL* proporciona una vía de comunicación con capas superiores (con el uso de TLS, por ejemplo) para la negociación de la sesión de autenticación. Los protocolos EAP y EAPOL no contienen algún sistema para la integridad o protección de la privacidad. De ello se

encarga el protocolo que emplee el servidor RADIUS, que garantiza los puntos antes mencionados.

EAP TLS

El mecanismo EAP TLS (EAP *Transport Layer Security*) es un algoritmo de autenticación proporcionado por Microsoft basado en el protocolo TLS. El TLS es una versión actual del *Secure Socket Layer* (SSL) que se emplea en la mayoría de los navegadores WEB para aplicaciones que implican transacciones de datos seguros.

TLS está diseñado para proporcionar la autenticación segura y la encriptación para una conexión segura TCP/IP. Se compone de tres partes: un protocolo de *handshake*, que se encarga de las negociaciones de la sesión SSL; un protocolo de registro, empleado para facilitar los intercambios encuitados entre el cliente SSL y el servidor; y por último un protocolo de alerta que se encarga de las notificaciones en autenticaciones exitosas o fallidas.

Así como esta modalidad, existen otras tantas que han sido desarrolladas por diversos fabricantes e implementados en sus propios productos. Por ello, se deja al criterio del administrador de red la implementación de éstos mecanismos.

## 5.5 El Estándar 802.11i

Uno de los objetivos principales del grupo de trabajo 802.11i es el definir una Red de Seguridad Robusta (RSN[16]). Dentro de una RSN, las asociaciones entre todas las estaciones incluyendo a los AP's, se construyen sobre una autenticación/autorización robusta denominada RSNA, la cual se define en el Estándar 802.11i como sigue: *la RSNA depende del IEEE 802.1X para transportar los servicios de autenticación y entregar los servicios de administración de llaves.*

El Estándar 802.11i define dos clases de estructuras de seguridad: RSNA y pre-RSNA. La diferencia entre estas dos estructuras se ve reflejada en el empleo de cuatro pasos adicionales (handshake) ejecutados por la estructura RSNA. Si un sistema no emplea estos cuatro pasos adicionales, se dice que la estación esta empleando la estructura pre-RSNA.

Pre-RSN

Este esquema consiste en dos subsistemas de seguridad: la autenticación de entidad 802.11 y el protocolo WEP. La autenticación de entidad incluye los sistemas de *Llave Compartida* y *Sistema Abierto.*

[16] Robust Security Network

RSN

Adicionalmente a los esquemas pre-RSN, la seguridad RSN define procedimientos de administración de llaves para las redes 802.11; también incrementa los procesos de autenticación y encriptación llevadas a cabo por la estructura pre-RSN.

- **Autenticación mejorada:** el Estándar 802.11i utiliza al 802.1X para la autenticación y los servicios de administración de llaves. Incorpora dos componentes dentro de la arquitectura 802.11: *Puerto y Servidor de Autenticación (AS) IEEE 802.1X*. El *puerto* representa la asociación entre dos puntos. Como se expuso anteriormente, el puerto que emplea el *802.1*X permitirá el tráfico de datos generales únicamente cuando la autenticación se ha completado satisfactoriamente. El AS puede ser un equipo separado o bien, estar incluido dentro del AP. Aunque no se recomienda el empleo de un protocolo entre el AS y el AP, deberá existir un canal seguro tal como el TLS o IPsec entre dichas instancias. Dado que el mecanismo EAP soporta la autenticación mutua, se deberá emplear dicho mecanismo dentro del esquema RSN, ya que el solicitante y el autenticador se autentican uno al otro.

- **Establecimiento y Administración de Llaves:** en el 802.11i se introducen dos formas de soporte a estas funciones: *administración manual y automática de llaves*. Como su nombre lo indica, la administración manual de llaves implica la intervención del administrador de red para la configuración de las llaves. La administración automática recae en el soporte que da el 802.1X, y específicamente a las cuatro formas de *handshake* que se emplean para cada transición de llaves.

- **Encriptación mejorada:** se desarrollaron dos algoritmos de encriptación avanzada, con el objeto de mejorar la confidencialidad de los datos: CCMP[17] y TKIP[18]. Dentro del esquema RSN, el algoritmo CCMP es reglamentario; en el caso del algoritmo TKIP se considera opcional y se recomienda solamente para cubrir las deficiencias del esquema pre-RSNA.

El IEEE 802.11i especifica el *Elemento de Información RSN (RSN IE*[19]*)* el cual contiene la información de seguridad que incluye las capacidades de la RSN en cuanto a la autenticación y la selección de llaves cifradas. El RSN IE puede ser empleado para distinguir a las estaciones que emplean los esquemas pre-RSN o RSN. Las estaciones que emplean el esquema RSN, deberán incluir el RSN IE en los frames tipo beacon, prueba-respuesta, solicitud de asociación y reasociación, y

[17] Counter-Mode/CBC-MAC Protocol
[18] Temporary Key Integrity Protocol.
[19] RSN Information Element

en los mensajes segundo y tercero de las 4 formas del *handshake* (que serán descritas posteriormente).

De manera general, el RSN IE contiene la información de la seguridad *robusta* que indica los algoritmos de autenticación y cifrado que serán empleados por los equipos del sistema de comunicaciones. Las estaciones y el AP pueden aprender las capacidades de seguridad de los puntos de comunicación y negociarlas entre ellos, gracias al RSN IE incluido en los frames antes mencionados. Posteriormente los procedimientos de seguridad serán ejecutados. En la siguiente figura se muestra un ejemplo del establecimiento de un esquema RSN entre el solicitante (estación) y el autenticador (AP) dentro de un BSS.

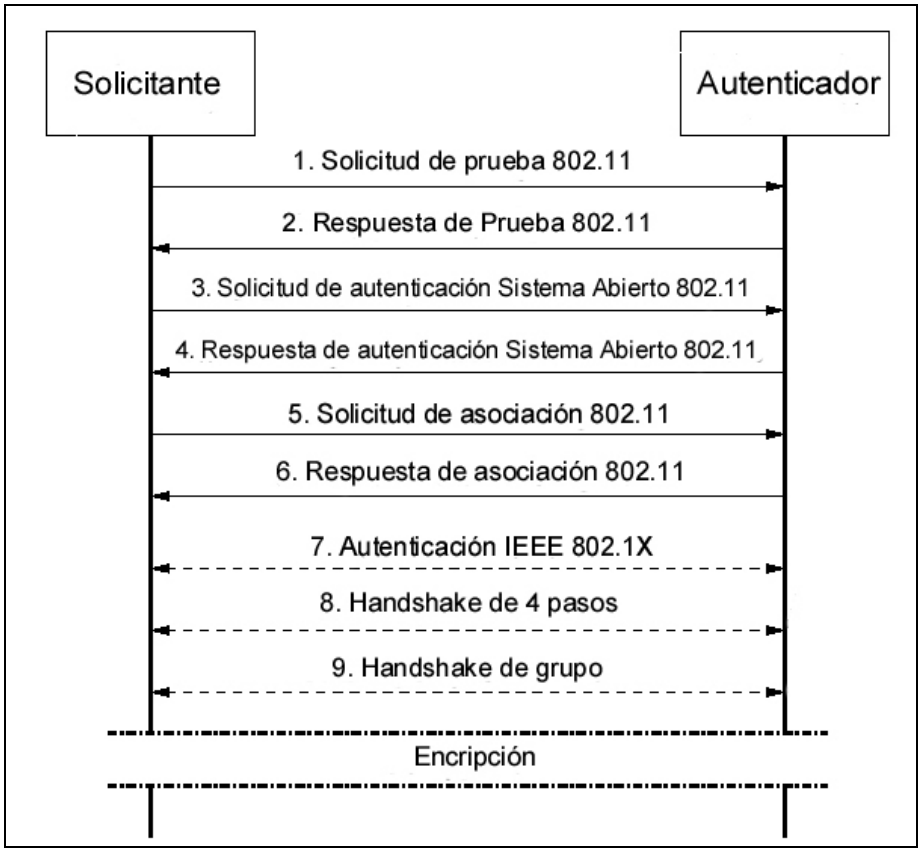



Figura 5.13
*Sesión de Autenticación en un Esquema RSN*

Después de que se ha llevado a cabo la autenticación tradicional (802.11), se inicia la parte correspondiente al 802.1X, que está representada en el paso 7. Los mensajes EAP serán intercambiados entre el solicitante, el autenticador y el servidor de autenticación (aunque no está representado en la figura). Si el solicitante y autenticador se logran autenticar mutuamente, ambos generarán de manera

independiente una *Llave Maestra Par (PMK*[20]*)*. El servidor de autenticación transmitirá la PMK al autenticador a través de un canal seguro (IPsec o TLS). El *handshake* de 4 pasos utiliza el PMK para derivar y verificar *la Llave de Transición Par (PTK*[21]*)*. De esta manera, se garantiza que la sesión de transmisión de la llave entre el solicitante y el autenticador se encuentra "fresca". Después de esto, se efectúa el handshake de grupo como se muestra en la figura. Dicho handshake de grupo, es empleado para generar la llave de grupo, que a su vez sirve para que los frames de tipo broadcast y multicast puedan ser intercambiados de forma segura.

Las siguientes secciones tratarán de las mejoras en cuanto a la autenticación, establecimiento y administración de llaves y encriptación, tal y como se define en el estándar 802.11i.

### 5.5.1 Mejoras en la Autenticación

En el Estándar 802.11 original, una estación deberá trabajar con un AP, luego entonces será capaz de acceder a los servicios WLAN. Un ejemplo de este proceso se encuentra en la figura anterior de los pasos 1 al 7. Como se expuso en las secciones anteriores, dentro de la asociación mediante el uso del Sistema Abierto no se maneja ningún algoritmo de autenticación. En el caso del mecanismo de Llave Compartida, éste no es adoptado por el Estándar 802.11i. En lugar de él se incorpora el esquema del 802.1X para establecer la solución RSN. Dicho estándar proporciona un *control de acceso basado en puertos* como mecanismo de control para proteger a la WLAN de usuarios no autorizados. El empleo de este mecanismo asegura la integridad del esquema RSN.

El Estándar 802.11i también especifica un esquema de seguridad más robusto empleando el *handshake de 4 pasos*, así como el *handshake de grupo* para autenticar y autorizar a las estaciones. Dichos esquemas serán discutidos en la siguiente sección.

### 5.5.2 Establecimiento y Administración de Llaves: Handshake de 4 pasos

El RSNA define un *handshake de 4 pasos* para llevar a cabo diversas funciones tales como verificar la actividad en la comunicación entre estaciones, garantizar el reemplazo constante de la llave de sesión, instalar la llave de encriptación así como su confirmación. El handshake de 4 pasos se lleva a cabo mediante el 802.1X. En específico, los mensajes intercambiados tienen el formato de llave EAPOL.

[20] Pairwise Master Key
[21] Pairwise Transient Key

En el handshake, el autenticador envía en primer lugar un mensaje al solicitante que contiene información de la llave y un *Anonce*. Un *anonce* es esencialmente un número pseudoaleatorio, el cual nunca es empleado de nueva cuenta. Después de que se recibe el primer mensaje, el solicitante valida el mensaje mediante la verificación del *Contador de Repetición (RC*[22]*)*. El RC es una secuencia de números que se incrementa durante cada mensaje llave EAPOL. Si el RC es menor o igual al valor almacenado en el solicitante, el mensaje será descartado por éste último. De otra forma, el solicitante genera un nuevo número llamado *Snonce*. Mediante el empleo de un algoritmo llamado Función Pseudo-Aleatoria (PRF[23]) con los valores del *Anonce*, *Snonce*, *PMK* y otros valores como entradas, el solicitante genera el valor PTK. El solicitante entonces envía de regreso el segundo mensaje conteniendo información de la llave, el *Snonce*, el RSN IE y el Código de Integridad del Mensaje (MIC[24]). El MIC es el compendio de la encriptación empleada para proporcionar el servicio de integridad.

Una vez que es recibido el segundo mensaje, el autenticador valida dicho mensaje revisando el RC. El proceso es similar al que ocurre cuando el solicitante recibe el primer mensaje. Es entonces cuando se deriva la PTK si se ha validado el segundo mensaje. Dado que el autenticador usa el mismo algoritmo y las mismas entradas, la PTK derivada del autenticador será la misma que generó el solicitante; el autenticador también verificará el MIC. El paquete será descartado si se trata de un MIC inválido. Adicionalmente, el autenticador compara el RSN IE que contiene con el recibido del solicitante de manera anticipada a la respuesta que se le enviará al solicitante; si los RSN IE no son idénticos se da por terminada la asociación. En caso contrario el autenticador envía el tercer mensaje al solicitante. Éste mensaje incluye información de la llave, el valor *anonce*, el MIC y el RSN IE del autenticador.

En la recepción del tercer mensaje, el solicitante verifica los valores del RC y del *anonce*. Después se comparan los valores del RSN IE que se recibieron con anterioridad en los frames Bacon o en los Prueba-Respuesta. El solicitante se *desasociará* de ese AP si el RSN IE es inválido. En el caso de que sea correcto, el solicitante procederá a revisar el MIC. Una vez concluida esta verificación, el solicitante manda un cuarto mensaje que contiene información de la llave y el MIC.

Cuando el cuarto mensaje se ha recibido por el autenticador, éste revisa el RC de forma similar a la revisión del mensaje tres. Si la nueva verificación el RC y el MIC resultan correctos, se concluye el handshake. El cuarto mensaje es usado para indicarle al autenticador que el solicitante ha instalado una llave temporal, PTK. La PTK sólo es conocida por el solicitante, el autenticador y el servidor de autenticación y sirve para encriptar los datos a transmitir.

[22] Replan Counter
[23] Pseudo-Random Function
[24] Message Integrity Code

### 5.5.3 Mejoras en la Encriptación

El algoritmo WEP es empleado como primer método de protección a la WLAN para mantener su confidencialidad. También es capaz de prevenir el acceso a la red sin autorización. El WEP está basado en la llave secreta compartida entre la estación y el AP. Emplea el esquema de cifrado RC4. Antes de enviar los datos, el remitente necesita procesar el valor (ICV) con el algoritmo CRC-32. El remitente entonces encripta los frames de datos y el ICV.

Se tiene conocimiento de que el protocolo WEP puede ser vulnerado. Esto se debe a la corta longitud del vector de inicialización (IV) y a la llave secreta estática. Los vectores de inicialización se emplean para concatenar la llave secreta compartida para producir diferentes secuencias para cada paquete. El IV es generado aleatoriamente y se incluye en los paquetes. Con una longitud de tan sólo 24 bits, WEP empleará eventualmente el mismo IV para diferentes paquetes, lo que se conoce como *colisión del IV*. Cuando se recolectan suficientes paquetes basados en el mismo IV, un atacante podría encontrar los valores contenidos en él. Por otra parte, dado que el Estándar 802.11 original no proporciona un mecanismo para la administración de llaves, el administrador de red y los usuarios en general emplean la misma llave compartida por un largo periodo de tiempo; incluso se comparte la misma llave WEP entre todas las estaciones del mismo BSS o ESS.

Para corregir los defectos anteriores del WEP, el Estándar IEEE 802.11i desarrolló un algoritmo mejorado llamado Protocolo de Integridad de la Llave Temporal (TKIP[25]). El TKIP inicialmente tenía el nombre de WEP2, ya que también está basado en la encriptación RC4. Sin embargo, se implementa de manera distinta de forma que atiende a las vulnerabilidades del WEP. El TKIP define una llave temporal (TK) que consiste en una llave secreta de 128 bits compartida entre el transmisor y receptor. Ambos emplean la misma cadena de ciframiento RC-4. Cada parte deberá cerciorase que no exista un valor de IV que se emplee más de una vez durante la TK actual. Se espera que el valor del IV sea implementado como un contador de 16 bits comenzando desde el valor cero.

Las implementaciones deben asegurarse de que la TK sea actualizada antes de que el espacio del IV se llene. TKIP también emplea un paquete llamado *contador de secuencia* con el fin de ordenar los MPDU's. Mas aún, el TKIP combina la llave temporal con la dirección MAC del dispositivo cliente, que resulta en un IV relativamente largo para producir la llave de encriptación. Esto asegura que cada equipo utilice una diferente llave.

Básicamente el TKIP aplica la misma encriptación que el WEP, pero hace uso del protocolo EAPOL 802.1X para actualizar las llaves temporales y prevenir la

[25] Temporal Key Integrity Protocol

reutilización de las llaves. Esto proporciona una distribución dinámica que mejora significativamente el desempeño de la seguridad proporcionada por el WEP. TKIP puede ser adaptado dentro de los productos existentes que operen bajo el estándar 802.11, únicamente será necesario actualizar el software que controla al esquema de seguridad. Adicionalmente, los equipos que sólo soportan el protocolo WEP, siguen siendo compatibles e interoperables con los equipos que trabajan en el esquema TKIP.

Además a la TKIP, el IEEE 802.11i también define el Protocolo Modo Contador/CBC-MAC (CCMP[26]), el cual consiste en una solución de larga duración. Y es considerada así porque emplea un esquema de encriptación más robusto, de manera que utiliza una llave de 128 bits, contrastando con los 32 bits de la TKIP. El CCMP requiere una nueva TK (llave temporal) para cada sesión y necesita refrescarla cuando se repite el paquete de números (PN). El PN es incrementado para cada MPDU y puede ser utilizado para prevenir un ataque cuando se reciba el Contador de Respuesta. El PN y el identificador de la llave se encuentran codificados en el encabezado CCMP. Aunque el CCPM puede proveer servicios de seguridad mucho más robustos, requiere de un hardware adicional (co-procesador) para mejorar el desempeño en la encriptación. Por ende, el viejo harware empleado en el estándar 802.11 puede no ser posible de actualizar.

[26] Counter Mode/Chipre Block Chaining - Message Authentication Code

CAPÍTULO SEIS

# Diseño y Propuesta de Implementación de la WLAN

## 6.1 Introducción

El diseño de una Red Inalámbrica WLAN implica considerar un conjunto de factores que no se contemplan en las redes convencionales. Es por ello que se debe hacer un esfuerzo adicional en el planeamiento de una nueva red WLAN debido a que son más diversas las causas que pueden contribuir al mal funcionamiento de la red o en la obtención de resultados no deseados.

Por ejemplo, un aspecto a considerar consiste en que en una red LAN, un mayor número de equipos dentro del sistema se traduce en un mejor desempeño, mientras que en una WLAN ocurre este fenómeno de manera inversa. Esto es debido a que mientras más equipos se encuentren en operación, mayor será la probabilidad de que dichos equipos se interfieran entre sí. Otro ejemplo consiste en que el diseño de la red se basa principalmente en valores teóricos tomados de las especificaciones del fabricante; sin embargo, existen varios estudios (además de experiencias en campo) que aseguran que no será fácil alcanzar dichos valores, porque son muy variadas las condiciones geográficas de los sitios donde se planea realizar instalación. Aunado a esto, no es sencillo contar actualmente con herramientas de medición que nos proporcionen datos confiables acerca de la potencia y calidad de señal transmitida por los puntos de acceso.

Para el diseño de la WLAN propuesta se deben considerar el mayor número de variables (que se han abordado a lo largo del presente texto) con el objeto de lograr el óptimo desempeño de la red. Por tal razón, a continuación se agrupan en categorías dichos factores con el fin de que sean más claros los aspectos a considerar en el diseño. En forma paralela se realiza el análisis de la mejor opción para el diseño de nuestra WLAN que atiende a las consideraciones mencionadas; dichas opciones se remarcan con las siglas ***WLAN FI***.

## 6.2 Propuesta de Diseño

### 6.2.1 Estándar a Utilizar

El primer paso para el diseño consiste en la elección del estándar bajo el cual operará la WLAN. Esto tiene que ver con el tipo de aplicaciones que se manejen en la actualidad o bien, aquéllas que se quieran implementar. De acuerdo al análisis de las tecnologías que se realizó en el capítulo 2, podemos resumir las características de los estándares que son empleados actualmente.

| Estándar | Frecuencia de Operación | Modulación | Cobertura Máxima | Tasa de Transmisión Máxima | Número Máximo de Canales sin Interferencia | Características Adicionales |
|---|---|---|---|---|---|---|
| 802.11b | 2.4 GHz | DSSS | 100m | 11 Mbps | 3 | Estándar más empleado en la actualidad |
| 802.11a | 5 GHz | OFDM | 50m | 54 Mbps | 12 | - |
| 802.11g | 2.4 GHz | OFDM | 100m | 54 Mbps | 3 | Compatible con los sistemas 802.11b |

Tabla 6.1
*Características Generales*
*de los Estándares 802.11 a, b y g*

El Estándar 802.11b debe ser considerado si:

- No se pretende emplear aplicaciones que requieran amplio ancho de banda.
- Se necesita tener cobertura en una zona de tamaño considerable.
- El precio es una consideración principal. Por ejemplo: el diseño de una red WLAN 802.11b cuesta aproximadamente una cuarta parte de lo que costaría implementarla bajo el estándar 802.11a, cubriendo la misma área con la misma tasa de transmisión.

La única desventaja del empleo de este estándar consiste en que la máxima tasa de transmisión que se puede alcanzar es de 11 Mbps. Por otra parte, la frecuencia de operación es la misma que emplean otros dispositivos que podrían causar interferencia.

El Estándar 802.11a debe ser considerado si:

- Las aplicaciones que se emplearán en la WLAN requieren de un amplio ancho de banda, tales como voz y video.

- Los usuarios se encuentran dentro de una región cercana (aproximadamente 50 m). El hecho de que hay más canales que no se sobreponen, permite la implementación de más AP's muy próximos entre si y sin interferencia entre ellos.

La principal desventaja del empleo de este estándar radica en que no es compatible con el 802.11b, que es el más popular actualmente y de bajo costo.

El estándar 802.11g debe considerarse si:

- Se necesitan correr aplicaciones que requieran un amplio ancho de banda y además se necesita cubrir una zona amplia.
- Se necesita compatibilidad con los equipos 802.11b

La principal desventaja del empleo de este sistema es que la tasa de transmisión disminuye cuando los esquemas 802.11g y 802.11b operan de manera simultánea. Por otra parte, enfrenta los mismos riesgos de interferencia que los sistemas 802.11b al emplear la misma banda de frecuencias: 2.4GHz.

***WLAN FI***

Para el diseño de red propuesta, considero que la mejor opción consiste en el empleo del Estándar 802.11g. Las razones son las siguientes:

- Permite la interoperabilidad con los sistemas 802.11b. Esto representa una ventaja para los usuarios que ya cuentan con los dispositivos compatibles con éste estándar. Los nuevos productos para el estándar 802.11g comienzan a comercializarse de manera considerable y por ende, los precios de estos productos tienden a la baja.
- A pesar de que la interoperabilidad de los sistemas 802.11b y 802.11g afecta la tasa de transmisión, ésta sigue siendo superior a la que alcanza el estándar 802.11b puro. Además de que el estándar 802.11g ofrece mayor tasa de transmisión, las características de la modulación empleadas por este sistema mejoran considerablemente la calidad de las transmisiones y optimizan el ancho de banda, lo que representa una ventaja adicional para los usuarios. Es de esperarse que los equipos tiendan a sustituir paulatinamente a los empleados actualmente bajo el estándar 802.11b, consiguiendo que finalmente se tenga una estructura 802.11g pura.
- Por último, el empleo del estándar 802.11g, deja abierta la posibilidad de extender el servicio a más usuarios con un impacto menor al que se tendría empleando una WLAN 802.11b. Hay que recordar que el total del ancho de banda que es capaz de manejar un AP, se divide entre el número de usuarios asociados con dicho AP. Mientras más ancho de banda esté disponible, podrá

ser mayor el número de usuarios que puedan emplear la red de manera simultánea.

### 6.2.2 Topologías de Red

De manera general, existen dos topologías principales en las WLAN's: Ad Hoc e Infraestructura. Para el caso de la red propuesta, es conveniente el diseño de una *Red tipo Infraestructura.*

***WLAN FI***

Este tipo de red será empleada como una extensión de la red LAN actual, lo que permitirá que dicha red sea administrada por los centros de cómputo que brindan servicio a la comunidad estudiantil.

A este tipo de diseño se le conoce también como diseño *centralizado*, ya que cada AP está controlado por una administración común. Esto representa una gran ventaja en la administración y actualización de los componentes de la red en materia de seguridad y/o en el empleo de nuevos estándares, pues basta con configurar un solo AP para que las modificaciones tengan efecto inmediato.

Un sistema centralizado también permite optimizar la administración del ancho de banda. Los administradores de red pueden organizar a la WLAN en dominios, garantizando el acceso y los privilegios a diferentes grupos de usuarios según lo requieran.

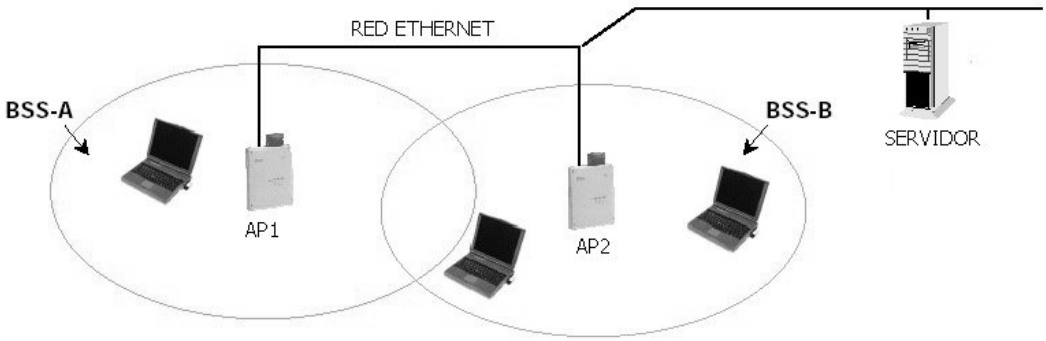



Figura 6.1
*Sistema WLAN Centralizado*

El tercer tipo de topología que consiste en el empleo de antenas direccionales, no es considerado debido a que no hay motivo para conectar mediante un enlace inalámbrico al Edificio Principal y el Anexo, dado que existe una red LAN en ambos edificios y es posible conectar nuestra WLAN a dicha red.

### 6.2.3 Definición del Número de Usuarios y Aplicaciones

Cuando se planea incrementar el número de usuarios y/o ancho de banda para una red existente, es conveniente realizar un análisis del tráfico con el objeto de que la propuesta de expansión sea la opción más adecuada. Adicionalmente, es necesario estimar el tipo de aplicaciones y el ancho de banda necesario para que la transmisión de datos se realice con el mejor desempeño posible.

Para este caso en particular, el diseño de la Red WLAN obedece más a una expansión en cuanto a número de usuarios, que a la necesidad de ampliar el ancho de banda. Por ello, se considera que el número de usuarios que se pretende considerar en un principio, no afectará de manera sustancial el desempeño de la red cableada actual, dado que los accesos a la WLAN compartirán las mismas aplicaciones que actualmente se brindan para los usuarios de la red cableada.

Para estimar el número de usuarios que inicialmente tendrán acceso a la WLAN, se realizó un sondeo entre la comunidad estudiantil de la Facultad de Ingeniería, que consiste en las siguientes 4 preguntas:

1. ¿Cuentas con un dispositivo portátil para el almacenamiento y administración de información? (Laptop, PDA, Palm, etc.? (SI/NO)

2. Si es afirmativa la respuesta anterior, ¿Dicho dispositivo cuenta con una interfaz compatible con la tecnología Wi-Fi? (SI/NO)

3. Si contaras con ambos equipos, ¿Te gustaría que la Facultad de Ingeniería brindara el servicio de red inalámbrica (WLAN)? (SI/NO)

4. ¿Está dentro de tus planes adquirir alguno de estos equipos a corto plazo (1 año)? (SI/NO)

La muestra consistió en un grupo de 100 alumnos divididos en 4 grupos de 25, correspondientes a las divisiones en las cuales están contenidas las carreras que se imparten en la Facultad de Ingeniería: División de Ingeniería Eléctrica, División de Ingeniería Mecánica e Industrial, División de Ingeniería Civil, Topográfica y Geodésica, y por último la División de Ingeniería en Ciencias de la Tierra.

Las respuestas se concentran en las siguientes tablas.

### División de Ingeniería Eléctrica

Muestra: 25 alumnos

| PREGUNTA 1 | | PREGUNTA 2 | | PREGUNTA 3 | | PREGUNTA 4 | |
|---|---|---|---|---|---|---|---|
| SI | NO | SI | NO | SI | NO | SI | NO |
| 5 | 20 | 4 | 21 | 25 | 0 | 7 | 18 |

### División de Ingeniería Civil, Topográfica y Geodésica

Muestra: 25 alumnos

| PREGUNTA 1 | | PREGUNTA 2 | | PREGUNTA 3 | | PREGUNTA 4 | |
|---|---|---|---|---|---|---|---|
| SI | NO | SI | NO | SI | NO | SI | NO |
| 8 | 17 | 3 | 22 | 25 | 0 | 5 | 20 |

### División de Ingeniería en Ciencias de la Tierra

Muestra: 25 alumnos

| PREGUNTA 1 | | PREGUNTA 2 | | PREGUNTA 3 | | PREGUNTA 4 | |
|---|---|---|---|---|---|---|---|
| SI | NO | SI | NO | SI | NO | SI | NO |
| 4 | 21 | 2 | 23 | 25 | 0 | 5 | 20 |

### División de Ingeniería Mecánica e Industrial

Muestra: 25 alumnos

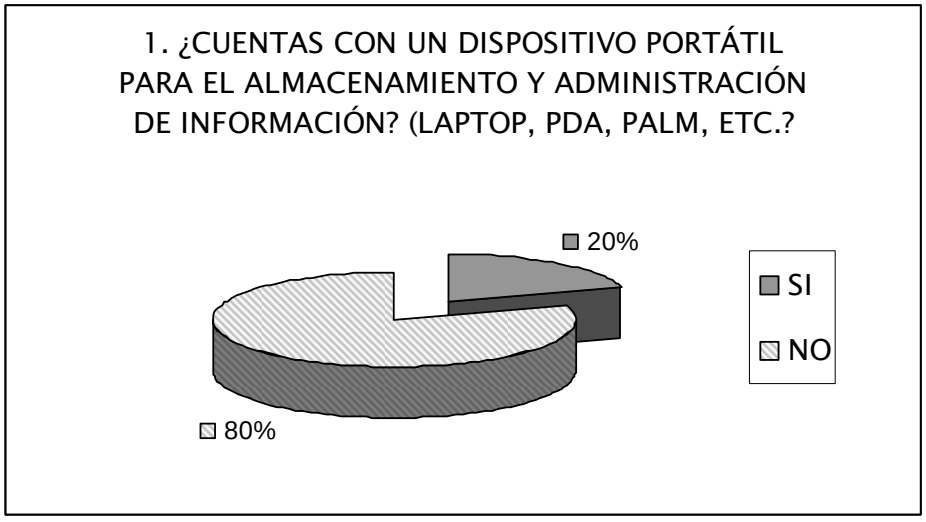
| PREGUNTA 1 | | PREGUNTA 2 | | PREGUNTA 3 | | PREGUNTA 4 | |
|---|---|---|---|---|---|---|---|
| SI | NO | SI | NO | SI | NO | SI | NO |
| 3 | 22 | 4 | 87 | 100 | 0 | 2 | 23 |

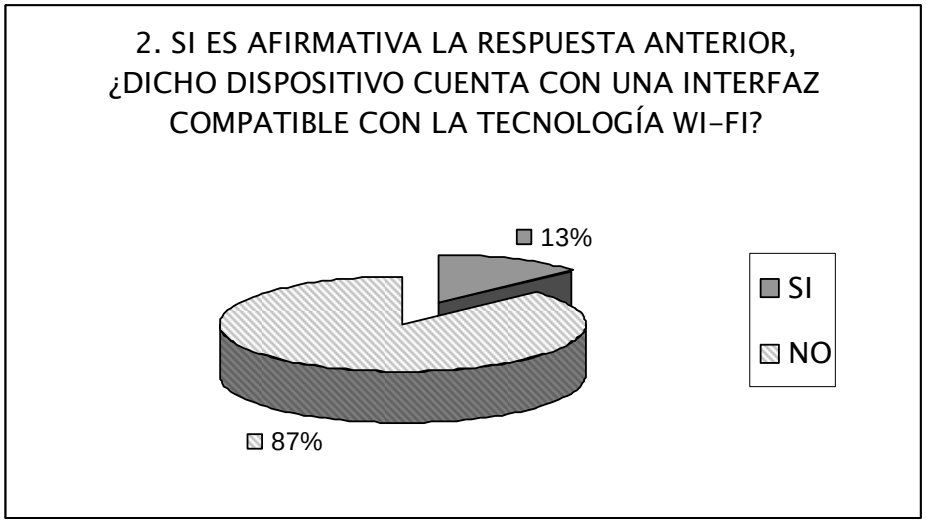
**Total de Respuestas**

Muestra: 100 alumnos

| PREGUNTA 1 | | PREGUNTA 2 | | PREGUNTA 3 | | PREGUNTA 4 | |
|---|---|---|---|---|---|---|---|
| SI | NO | SI | NO | SI | NO | SI | NO |
| 20 | 80 | 13 | 87 | 100 | 0 | 19 | 81 |

Las siguientes gráficas representan en términos de porcentajes totales, los resultados obtenidos.





De acuerdo al Informe 2003, la Facultad de Ingeniería cuenta con una matrícula de 8963 alumnos, incluidos los de primer ingreso. La muestra que se realizó para conocer el número de alumnos que cuentan con un dispositivo con posibilidades de tener acceso a una WLAN fue de 100 alumnos, lo que representa una muestra del 1.11 % de la población total.

Las gráficas mostradas en el anteriormente, nos hacen inferir lo siguiente:

1. Respecto a la primera pregunta, el 20 % cuenta con un dispositivo que podría ser empleado bajo un ambiente WLAN. Por tanto, se estima que un total de 1790 alumnos cuentan con dicho dispositivo.

2. Respecto a la pregunta 4, del total de alumnos que no cuentan con ningún tipo de dispositivo Wi-Fi (7170), el 19% adquirirá uno de estos equipos dentro del próximo año, de lo cual podemos inferir que 1362 alumnos contarán con dicho equipamiento.

La información anterior nos muestra que para el próximo año, se estima que serán 3152 alumnos los que contarán con un dispositivo Wi-Fi compatible. En términos estadísticos, esto representa un 35% de la población total.

Esta estimación resulta bastante optimista dado que la muestra empleada para realizar la encuesta fue considerablemente pequeña. Sin embargo, nos da una idea clara de que la tecnología de vanguardia resulta cada vez más accesible a los grupos estudiantiles y para este caso, para los alumnos de la Facultad de Ingeniería.

Por otro lado, analicemos el estado actual de la red de cómputo de la Facultad de Ingeniería. En conjunto, los Laboratorios de Cómputo UNICA y de la DIE-DIMEI cuentan con aproximadamente 400 computadoras disponibles[1] para los alumnos. Algunos de éstos, son para uso exclusivo de algunas carreras, materias o cursos especializados. De acuerdo a mis observaciones, estos laboratorios cumplen con los objetivos para los cuales están diseñados. Sin embargo, en algunas ocasiones no resulta sencillo poder acceder a estos servicios debido a la sobre demanda en ciertos horarios y etapas del ciclo escolar; por ejemplo, dentro del horario de 2 a 4 pm (en el cual no hay clase regularmente) y en el periodo final de cada semestre.

Ésta es parte de la necesidad detectada que impulsa de manera principal el desarrollo de este proyecto. Ya se demostró que parte de la población es capaz de recibir el servicio de red inalámbrica. Si ésta es llevada a cabo, se resolverían dos de las problemáticas mencionadas con anterioridad:

1. Tomando en cuenta que los alumnos poseen dispositivos compatibles con Wi-Fi, **se pretende descongestionar los centros de cómputo brindando el servicio WLAN en las áreas libres**. De esta manera, se aprovecha que los alumnos que cuentan con un dispositivo móvil, no requieran acudir a los centros de cómputo para realizar sus actividades académicas y esto tiene su beneficio directamente con la disminución del número de usuarios en dichos centros.

2. La ventaja que se tiene en la WLAN para los espacios abiertos, es que no se requiere un lugar fijo para poder asociarse con un AP. Esto implica de manera ideal, que se podrán asociar tantos usuarios como espacio libre se disponga. Además, no será necesario invertir en nueva infraestructura para

[1] De acuerdo al conteo realizado sobre los esquemas de Red proporcionados por los coordinadores de cada laboratorio citado.

acondicionar nuevos espacios. Bien se podría analizar la propuesta de implementar algunas mesas de trabajo, pero esto con el carácter de opcional.

Ahora bien, una de las principales limitaciones para determinar el número de usuarios que simultáneamente pueden asociarse a un AP, dependen de lo siguiente: modelo del AP a utilizar, la capacidad de la red actual para soportar al AP (es decir, puertos libres y compatibilidad entre los dispositivos), el espacio físico disponible y el tipo de tráfico que se requiere para ejecutar las tareas académicas cotidianas.

A través de la información proporcionada por los Administradores de los Centros de Cómputo es posible conocer los dispositivos que actualmente están funcionando para darle el soporte necesario a la red cableada. De acuerdo a los manuales de estos equipos, se sabe que son compatibles con los AP's propuestos porque cumplen las siguientes características: los puertos de los switches tienen la característica de autonegociación y operan a la misma velocidad que los AP´s propuestos; los switches soportan los protocolos de seguridad que están integrados en los AP´s; y por último, existen puertos disponibles en los switches para conectar uno o más AP's.

El número de usuarios que un AP puede manejar varía desde 1 hasta 253 usuarios simultáneos[2]. Esta cifra es variable de acuerdo a las condiciones geográficas y al tipo de tráfico que se demande. Se estima que la ubicación propuesta, el número de usuarios y las condiciones geográficas en las cuales operarán los AP's, no representarán motivos sustanciales para que el rendimiento de la WLAN se vea afectado.

### Definición de Aplicaciones

Por último, mencionamos con anterioridad que las aplicaciones académicas actuales no se consideran críticas, es decir, no manejan tipos de tráfico como lo son voz o video. Estos servicios requieren un mínimo de ancho de banda para asegurar que los datos lleguen a su destino (QoS)[3], pero el flujo de información que comúnmente requieren los alumnos se limita a la transmisión de datos. Esto hace que la administración del ancho de banda sea lo suficientemente flexible y de ésta forma, no se limita el número de usuarios (pero bajo el riesgo de que mientras mayor sea el número de usuarios, la velocidad de transmisión decrecerá de manera proporcional, además de que también es mas grande la probabilidad de que se produzcan colisiones, produciendo mayor lentitud en el sistema).

Para administrar de mejor manera el ancho de banda, se pueden definir VPN's sobre las cuales se identifique a las aplicaciones que consumen demasiado ancho de banda y de ésta manera, evitar que un solo usuario afecte el desempeño de la red.

[2] Access Point 3COM 8750
[3] Quality of Service

En base a la información anterior, se estima que las capacidades de los AP's propuestos podrán satisfacer adecuadamente las necesidades de los usuarios por lo siguiente:

- El número de usuarios que simultáneamente accederán a los servicios que la WLAN proporcione, no excederá de 50 usuarios por AP, esto debido a que los espacios propuestos no poseen la capacidad para tal estimación.

- Por otra parte, la estimación de 50 alumnos simultáneos para cada AP (considerando que se instalarán 3 AP) resulta adecuada contrastada con el número de usuarios que emplean computadoras de escritorio ubicadas en los centros de cómputo, pues hemos mencionado que existen alrededor de 400 lugares disponibles. Con esta acción, se podrían atender a 150 alumnos que representarían el 37.5 % de los usuarios de los centros de cómputo actuales.

Por todo ello, podemos manejar la cifra de 50 alumnos (inicialmente) como límite de usuarios que podrán emplear la red WLAN de manera simultánea para cada espacio propuesto (o bien, por cada AP). Este número puede variar de acuerdo a las observaciones que el administrador de red realice una vez que la WLAN se encuentre operando y puede ser modificado según se requiera.

### 6.2.4 Estudio del Sitio y Cobertura

#### 6.2.4.1 Estudio del Sitio

La propuesta que presenta este documento, abarca tres diferentes zonas de cobertura, una de ellas ubicadas en la planta baja  Edificio Principal y las otras dos en el ala norte del Anexo de la Facultad de Ingeniería y en la explanada principal respectivamente.

El estudio del sitio consiste en el análisis de los distintos factores ambientales que estarán interactuando con la red WLAN. En otras palabras, todos aquellos elementos que se encuentran dentro del área de cobertura, como son: paredes, techos, columnas, otros dispositivos inalámbricos, etc. Para determinar cuales serían los posibles factores que afectarían el desempeño de nuestra red, se selecciona la ubicación de los AP's para posteriormente analizar las ventajas y desventajas de dicha ubicación. La ubicación de los puntos de acceso obedece principalmente a dos factores:

- **Condiciones geográficas:** Es importante considerar los obstáculos, así como otros puntos de acceso y dispositivos que puedan interferir en la operación óptima del AP en cuestión.

- **Cobertura del AP:** Una vez que se ha determinado la posición ideal del AP, es importante conocer el área que el AP será capaz de cubrir de manera ininterrumpida o al menos, con la menor cantidad de obstáculos. En este aspecto, también influye el patrón de radiación de las antenas del AP. Existen muchos modelos con antenas de tipo direccional y omnidireccional, lo que afecta de manera sustancial la ubicación de los AP's.

En un principio estamos considerando los espacios abiertos para brindar el servicio de red. Los obstáculos que se presentan en estas áreas se componen únicamente de árboles. Para saber que tanta atenuación es provocada por éstos, sería conveniente realizar pruebas de potencia con las herramientas adecuadas para tal propósito. Sin embargo, en base a la información proporcionada por los proveedores de los equipos que se proponen en la segunda sección de este capítulo, consideramos idealmente que la atenuación no tendrá un impacto significativo en el desempeño de la red. Otro punto importante se encuentra en los propios estudiantes. Éstos estarán en continuo movimiento, provocando absorciones y reflexiones de la señal, dando origen a la atenuación y multitrayectorias. Afortunadamente, los métodos de modulación y codificación ofrecen mecanismos confiables para contrarrestar éstos efectos. Se contemplan las siguientes áreas para contar con los servicios WLAN[4]:

[4] Las respectivas plantas de conjunto serán tratadas en la sección denominada "Interconexión con la WLAN"

Zona de Cobertura 1. Edificio Principal

## Zonas de Cobertura 2. Edificio Anexo Norte

Zonas de Cobertura 3. Edificio Anexo Sur

Otra consideración no menos importante radica en la ubicación de la red LAN, porque en ésta estaría constituido el principal soporte a la red WLAN. Sería inconveniente colocar un AP a una distancia considerable de la red cableada, pues la conexión por cable entre estos dos elementos de la red está sujeta a una atenuación muy grande.

Afortunadamente, existen en el mercado productos de cableado que ofrecen una baja pérdida, con una longitud máxima de 100 ft (30 metros), lo que es suficiente para que nuestro AP pueda conectarse a los equipos de red ubicados en los centros de cómputo.

Una vez que se ha decidido parcialmente la ubicación de los puntos de acceso, necesitamos contar con un Switch para tener la interconexión con la red LAN.

Partiendo de lo anterior se deberá realizar el siguiente procedimiento:

- Realizar los cableados de UTP desde el sitio donde se encuentra el punto de acceso hasta el switch. Ésta propuesta contempla a los laboratorios de UNICA y PROTECO como proveedores de interconectividad entre la red LAN y la WLAN.

- Colocar de manera provisional el punto de acceso en el sitio seleccionado.

- Realizar las pruebas necesarias para verificar que la ubicación del punto de acceso cumple con los requerimientos definidos, en caso de no ser así de debe reubicar a un sitio donde dichos requerimientos se satisfagan. En este punto se definirá la potencia de transmisión.

- Una vez satisfechos todos los requerimientos se fija de manera definitiva el punto de acceso.

#### 6.2.4.2 Interferencia y Atenuación

Interferencia

Existen dos factores principales por los cuales el desempeño de las WLAN's puede resultar afectado debido a la interferencia:

a) Las bandas de frecuencia que emplean las WLAN's no requieren de licencia alguna, por lo que los usuarios y/o administradores de la red no cuentan con un canal privado para la comunicación de sus equipos, es decir, pudiera darse el caso de que compartan un mismo medio con otras WLAN's.

b) Existen varios productos de uso doméstico que operan en las mismas bandas de frecuencia que las WLAN. Por tal motivo, ambos sistemas pueden interferirse entre sí.

El problema de la interferencia con las redes existentes puede solucionarse mediante la propuesta de distribución de células bajo el mismo esquema que una red celular, tal y como se describe en la siguiente sección.

Una vez que se ha definido el canal en el cual operará nuestra red, el proceso para la implementación de más AP's seguirá el mismo esquema propuesto, siempre y cuando se realicen las mediciones que sean necesarias para evitar los problemas que surgen en el área de cobertura que tratamos en el inciso correspondiente.

Para nuestro caso, la influencia de aparatos domésticos y específicamente los hornos de microondas, deben ser considerados ya que ambos sistemas comparten el espectro de frecuencias de 2.4 a 2.4835 GHz, y también porque es un dispositivo de uso bastante común dentro de las instalaciones de la Facultad de Ingeniería.

Las WLAN's pueden trabajar en los sistemas DSSS, FHSS, OFDM y esquemas híbridos. Los efectos de la interferencia causada por otros dispositivos varía según el sistema empleado y son tratados a continuación.

**Interferencia en Sistemas DSSS**

La interferencia en los sistemas DSSS es totalmente diferente a la que ocurre en los sistemas FHSS. A diferencia de éste último, los sistemas DSSS emplean una sola frecuencia para transmitir y recibir, ocupando un ancho de banda de 20 MHz, y a pesar de que se puede emplear una frecuencia específica para el intercambio de datos, existe la probabilidad de que otros dispositivos interfieran en la frecuencia de operación de los sistemas que emplean el esquema DSSS.

El peor escenario que se contempla consiste en que un dispositivo (por ejemplo un horno de microondas) se encuentre operando en la misma banda de frecuencia que la red WLAN.

A pesar de que esta situación puede presentarse, la confiabilidad del sistema es hasta cierto punto dependiente de la longitud de los paquetes. En estudios realizados[5] se ha demostrado que paquetes pequeños tienen una alta tasa de error EBR cercana al 50%. Para paquetes de longitud de 100 bytes, el EBR baja hasta un 10% con un Eb/Jo cercano a -1 dB. Para paquetes de mayor tamaño (mas de 2500 bytes) el Eb/Jo baja hasta 0.5 dB. La razón de este efecto radica en que la portadora del sistema DS no es suprimida por la interferencia. En la experiencia se ha

[5] Effects of Microwave Interference On IEEE 802.11

demostrado que los receptores de DSSS pueden operar muy próximos a los hornos de microondas manteniendo tasas de transmisión razonables.

**Interferencia en Sistemas FHSS**

Los sistemas FHSS dividen al ancho de banda disponible en 75 canales o *slots*. Durante la transmisión de una señal FHSS, existe la posibilidad de que un slot ocupe exactamente la misma frecuencia que un dispositivo ajeno a la WLAN. Esta situación cuenta con dos variantes:

a) El canal ocupado por el dispositivo externo interfiere sólo en breves periodos durante la transición del estado encendido-apagado. En este caso, dependerá del tamaño de los paquetes que maneje la WLAN, ya que si se trata de paquetes más grandes que la duración de la transición del dispositivo que interfiere, no será posible evitar dicha interferencia.

b) El canal ocupado por el dispositivo externo se encuentra en estado estacionario. Para este estado (que sería el peor de los casos), la interferencia ocurrirá solamente en un canal. Sin embargo, debido a que este sistema emplea diferentes frecuencias durante la transmisión de los datos, existirán pérdidas de paquetes aleatoriamente y no afectará a un usuario en específico; dichos paquetes pueden ser recuperados en una transmisión posterior y sin ocupar el canal interferido.

Como conclusión a estos puntos, podemos asegurar que los dispositivos que se encuentran dentro de las instalaciones de Facultad y que comparten la misma frecuencia con la WLAN, no tendrán un impacto sustancial en el desempeño de la red debido a lo siguiente:

- Los AP's propuestos emplean el esquema de modulación DSSS para el caso del Estándar 802.11b y por ende, los efectos de la interferencia no son considerables.
- La ubicación de los puntos de acceso y de los usuarios quedan fuera del alcance de estos dispositivos (con excepción de una zona). En el supuesto de que se presentara este caso, la justificación en los puntos anteriores nos permite seguir adelante con el diseño propuesto.

Atenuación

La atenuación se debe principalmente a los siguientes factores:

- Muros de concreto.
- Muros con superficies metálicas.
- Distancias muy largas entre el AP y el usuario, así como una mala administración de la potencia te transmisión.

De manera específica y aplicado a las zonas en las que se pretende instalar las WLAN's, se considera lo siguiente:

- Las superficies metálicas causan atenuación y reflexión, provocando que la señal no sea recibida con la misma intensidad en diferentes sitios aún estando a la misma distancia del Punto de Acceso.
- Los muros y techos pueden ocasionar atenuación si son de concreto, o si tienen armado de varillas metálicas en su interior, por lo que este tipo de estructuras también deben ser tomadas en cuenta, considerando sus dimensiones y su ubicación exacta.
- Otras fuentes de atenuación son los conductos de aire acondicionado, las cañerías metálicas, las instalaciones eléctricas y aditamentos como lámparas fluorescentes.

Los puntos mencionados anteriormente siempre deben ser incluidos como parte de una solicitud de red inalámbrica antes del diseño, ya que existen casos en los cuales es imposible instalar una red inalámbrica por factores tales como la atenuación.

Desafortunadamente, la única forma de combatir los problemas de atenuación e interferencia consiste en analizar detalladamente el entorno donde se planea implementar los AP's y si es posible, realizar las pruebas que sean necesarias.

Las redes inalámbricas son una tecnología relativamente nueva y hasta la fecha no existe la instrumentación necesaria para calcular con exactitud el impacto que las fuentes de interferencia y atenuación ocasionan a una red de este tipo instalada en un edificio determinado.

Sin embargo, emplearemos los elementos teóricos que se encuentran disponibles con el objeto de realizar un diseño que sea lo más real posible y considerando los efectos que pudieran ocasionar los factores externos. Además, reitero que el espacio propuesto es un espacio libre, y por tanto, los problemas antes mencionados carecerán de impacto relevante en el diseño propuesto.

#### 6.2.4.3 Cobertura

En los sistemas inalámbricos es indispensable que los equipos que pertenecen a la red, se encuentren dentro de una misma área de cobertura. Se definirán entonces las condiciones para que esto se lleve a cabo con éxito.

Para los equipos WLAN se establece un umbral de potencia mínima de recepción para considerar a una señal procedente de otro equipo como válida. La potencia de transmisión por lo general es variable, lo cual tiene su impacto en el hecho de que dos dispositivos que se encuentren trabajando en dicho sistema, no garantiza que puedan comunicarse entre sí. Para que esta comunicación sea exitosa, depende de

que los equipos puedan escuchar apropiadamente la señal de otro, por ejemplo: si un equipo "A" puede distinguir la señal de "B", pero "B" no pude distinguir la de "A", no habrá comunicación entre ellos. Por tal motivo, para que la comunicación sea posible se requiere:

- ✓ Que ambos equipos estén lo suficientemente cerca para que el primero pueda distinguir la señal del otro.
- ✓ Que transmitan a potencias suficientes para distinguir su señal mutuamente a pesar de la distancia y obstáculos entre ellos.
- ✓ Que sus antenas tengan la ganancia suficiente para recuperar la señal sobre el ruido de fondo, independientemente de la potencia de transmisión y de la distancia entre ellos.

Los dispositivos WLAN emplean la misma antena para transmitir y para recibir. No obstante, el área que cubre un dispositivo por su potencia de transmisión (donde los demás lo pueden escuchar adecuadamente) no necesariamente es igual a la que cubre por su sensibilidad de recepción (el radio alrededor de él donde puede escuchar a otro dispositivo que transmite). Por ejemplo un dispositivo puede "escuchar bien" a cualquier otro que esté en un radio de 100 metros a su redonda, pero su transmisión solo cubrir un radio de 40 metros alrededor de él.

Para ejemplificar las consideraciones anteriores, se supondrá un caso ideal en el que cada uno de los dispositivos involucrados "escuchan bien" y transmiten de igual forma en un radio alrededor de sí mismo; el área que define el radio se le denominará *área de cobertura.*

Se define que un dispositivo WLAN (punto de acceso o cliente inalámbrico) sólo podrá ser escuchado por otro dispositivo dentro de su área de cobertura; de igual forma, un dispositivo sólo podrá escuchar la señal de otro dispositivo dentro de su propia área, en la siguiente figura se ejemplifica lo anterior.

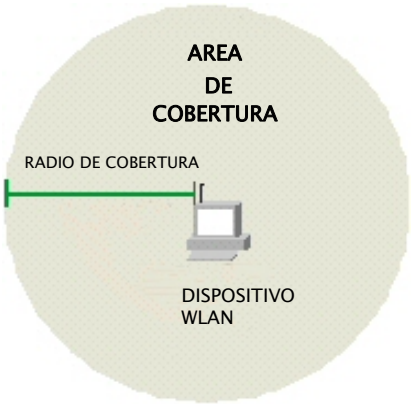



Figura 6.2
*Definición del Área de cobertura*

La condición para que se comuniquen dos dispositivos inalámbricos se ilustra en la siguiente figura:

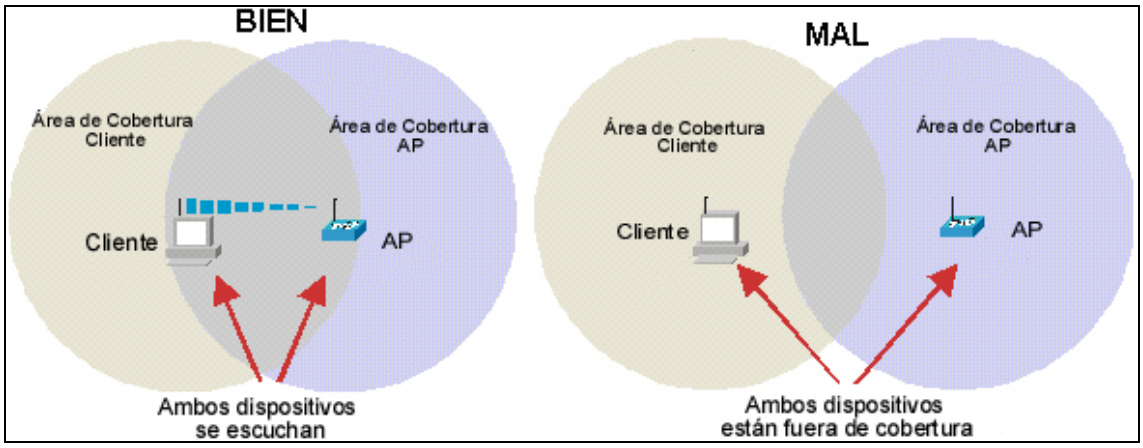



Figura 6.3
*Condiciones mínimas para la Comunicación*

En una WLAN en modo infraestructura, toda la comunicación se da entre los clientes y un punto de acceso. Si se requiere una comunicación entre clientes A y B, ésta primero tiene que pasar por el punto de acceso, por tanto el punto de acceso es el dispositivo más activo de la red.

En un entorno donde hay más de un punto de acceso un cliente puede tener sólo una conexión con un punto de acceso, para ello es necesario que el cliente se asocie lógicamente con uno de los puntos. Como consecuencia un cliente no puede estar asociado a más de un punto a la vez.

Los puntos anteriores definen de que manera se logra la comunicación exitosa entre dos o más dispositivos. Ahora se procederá a explicar los problemas que enfrentan los dispositivos WLAN y sus consecuencias.

### Problema de los puntos de acceso muy próximos entre sí

Si dos puntos de acceso (AP) trabajan con el mismo canal y cada uno está dentro del área de cobertura (AC) del otro, se interferirán continuamente debido a que ambos puntos generan una gran cantidad de tráfico y emplean las mismas frecuencias; por lo tanto el desempeño de la transmisión será afectada notablemente como sucede en una red Ethernet con un gran número de colisiones. En la siguiente figura se ilustra este problema:

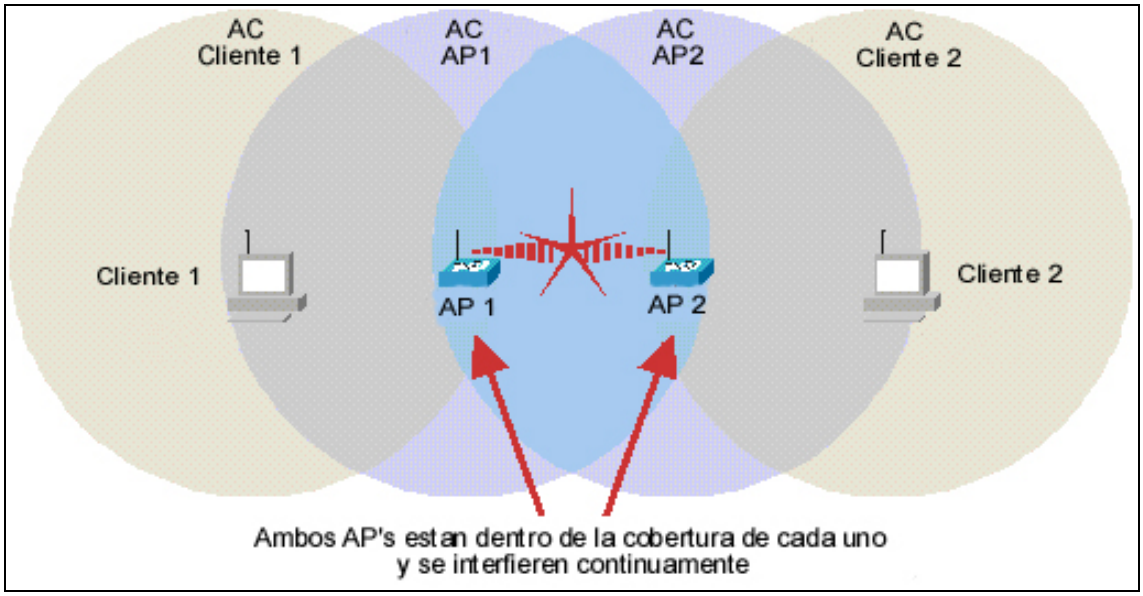



Figura 6.4
*Problema de Nodos muy próximos entre sí*

## Problema del nodo oculto

Este problema ocurre cuando un punto de acceso queda entre dos clientes, y ambos están dentro del área de cobertura del punto de acceso al que están asociados por ser el más cercano. Cuando el cliente A está transmitiendo hacía el punto de acceso que escucha, el cliente B no pude escuchar al A por la distancia entre ellos, por lo que supone que el medio está libre e inicia su transmisión.

La transmisión alcanza al punto de acceso que ahora no puede distinguir la información que recibe por su antena y entonces se produce una colisión. Ni A ni B pueden escucharse debido a que ambos están fuera del área de cobertura del otro, por lo que seguirán transmitiendo hasta que el punto de acceso les informe a ambos que hubo una colisión, momento en que volverán a esperar un intervalo aleatorio para transmitir, esto causará que transmitan la totalidad del paquete sin saber que han colisionado.

## Problema del nodo expuesto

En esta situación los puntos de acceso están lo suficientemente lejos entre sí para que se interfieran el uno al otro, no obstante entre ellos hay una superposición entre sus áreas de cobertura de tal forma que los clientes que quedan dentro de esta superposición pueden asociarse con cualquiera de ellos en forma estocástica. La asociación será sólo con uno, pero las transmisiones del cliente (independientemente de con que punto de acceso se haya asociado), serán escuchadas por ambos puntos de acceso, lo cual puede considerarse como una colisión porque mientras el cliente se encuentre transmitiendo, ninguno de los

puntos de acceso podrá transmitir o recibir la transmisión de ningún otro cliente aún cuando se supone que se cubren áreas distintas.

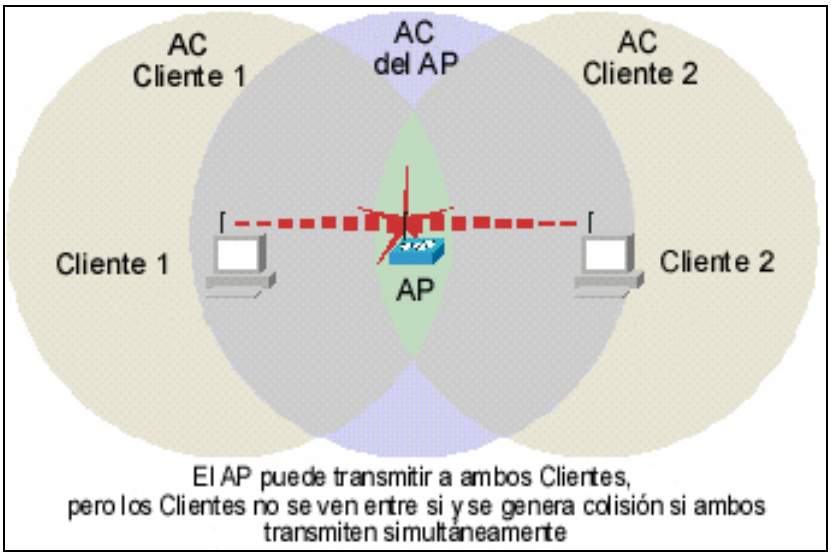



Figura 6.5
*Problema del Nodo Oculto*

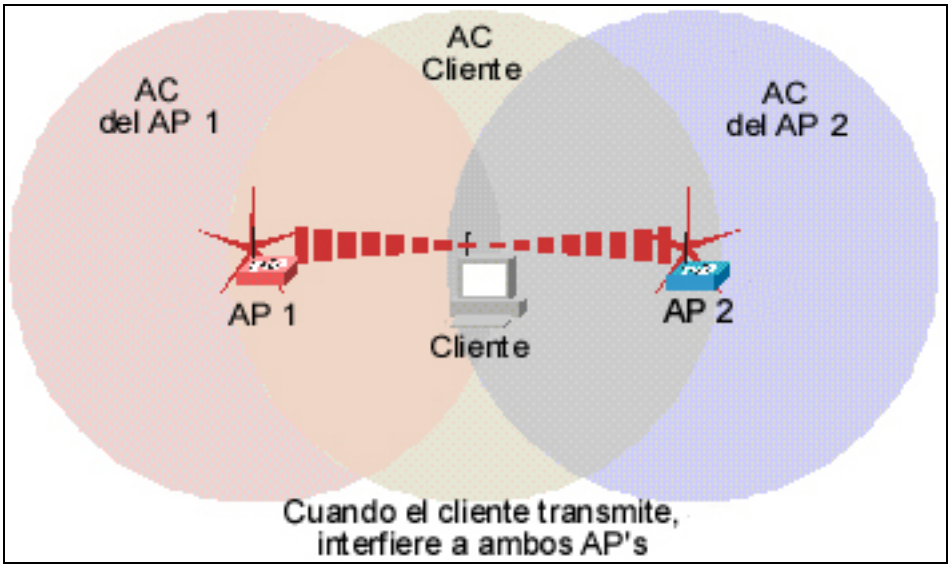



Figura 6.6
*Problema del Nodo Expuesto*

## Falta de cobertura

Si un cliente queda fuera del área de cobertura de un punto de acceso debido a que se encuentra a distancia grande de cualquier punto o bien, porque las características de los edificios adyacentes atenúan por abajo del umbral de recepción la

transmisión que llega al cliente, dicho cliente quedará incomunicado y no podrá asociarse con ningún punto de acceso. Por otra parte si el cliente queda muy lejos del punto de acceso, la comunicación no será mayor a 1 Mbps todo el tiempo.

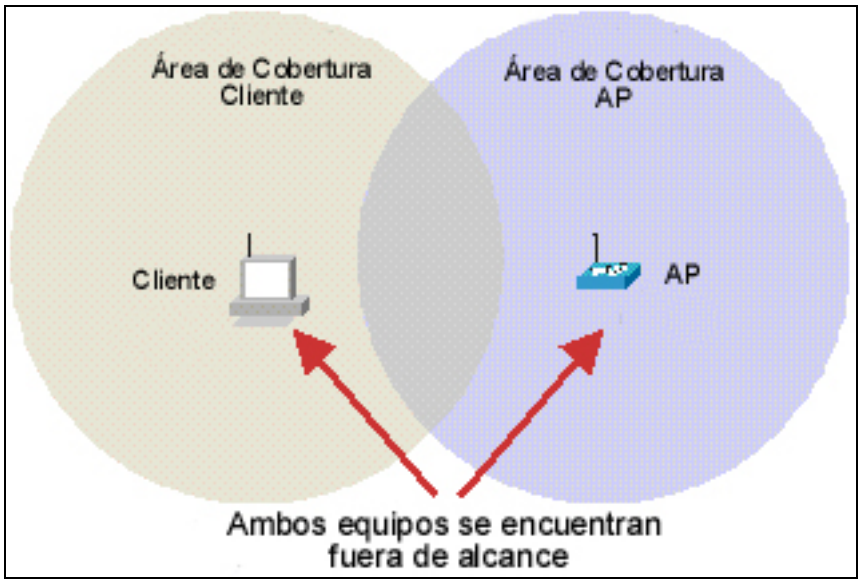



Figura 6.7
*Problema de la Falta de Cobertura*

Estos problemas demuestran que es crítico el ajuste de las potencias de transmisión y los umbrales de recepción así como la posición de los dispositivos y las distancias entre los puntos de acceso. A continuación se proporcionan una serie de recomendaciones para disminuir el impacto de dichos problemas de acuerdo a nuestro proyecto.

Se debe tratar de ajustar la potencia de transmisión de los dispositivos pertenecientes a un punto de acceso determinado (incluido él mismo) y los umbrales de recepción de tal forma que el área donde puede escuchar un dispositivo sea igual al área donde puede ser escuchado, en caso de que estos parámetros no se puedan ajustar directamente, se deben seleccionar las antenas adecuadas para fijarlos en forma indirecta.

Para evitar el problema del cliente oculto es deseable que todos los clientes se posicionen lo más cerca posible de sus respectivos puntos de acceso y que estén colocados de forma que todos queden dentro de las áreas de cobertura de todos los demás para que todos "se escuchen" entre sí, disminuyendo significativamente la duración de las colisiones. En la siguiente figura se ilustra la colocación ideal de los clientes alrededor del punto de acceso.

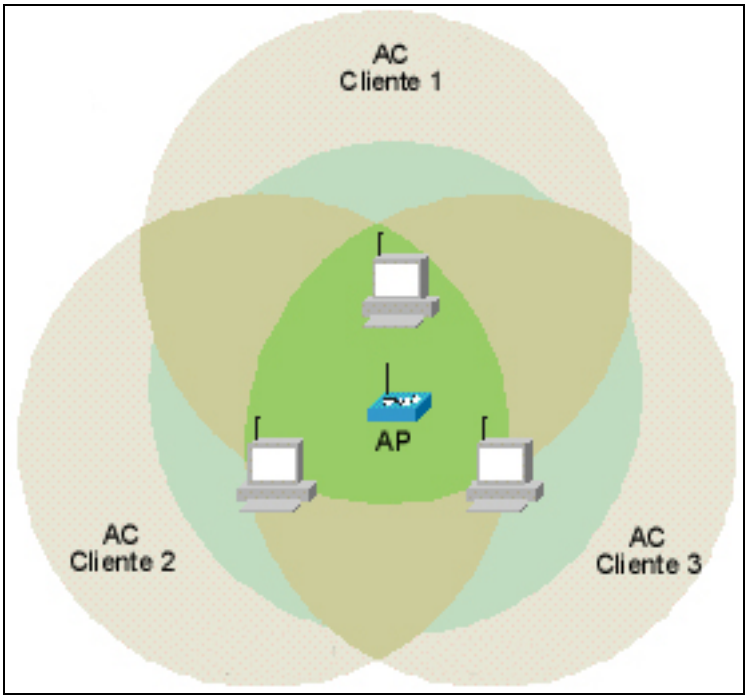



Figura 6.8
*Cobertura Ideal*

Para evitar el problema del cliente expuesto se debe asegurar que el área de cobertura de los clientes que pertenecen a un punto de acceso, no cubra a ningún otro punto de acceso y de preferencia tampoco a ningún cliente que no pertenezca a su propio punto de acceso como lo ilustra la siguiente figura:

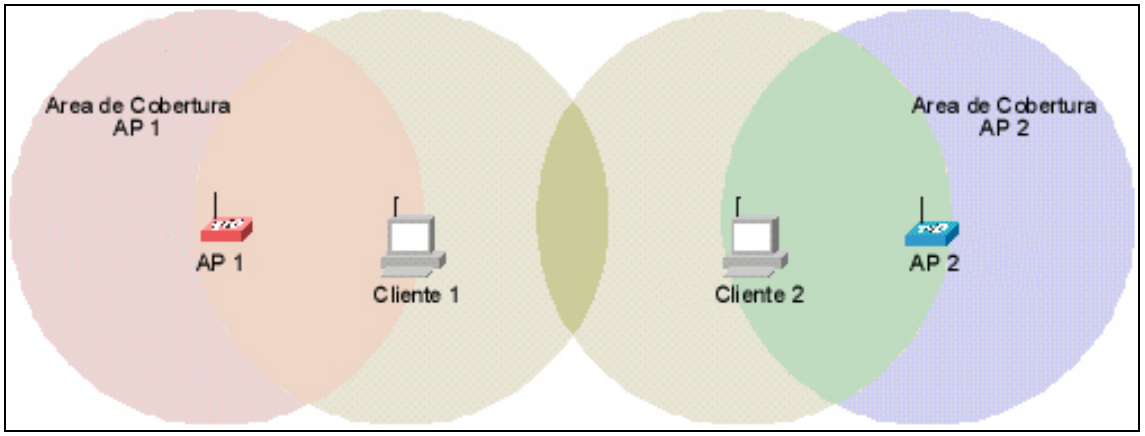



Figura 6.9
*Distancia Apropiada entre AP's*

***WLAN FI***

Para nuestro diseño se tiene que existen dos problemas que ocasionarían un desempeño no deseado de la WLAN: el problema del nodo expuesto y la falta de cobertura. El problema del nodo expuesto es resuelto mediante una adecuada configuración del mecanismo CTS/RTS.
La apropiada configuración de éste protocolo opcional puede ayudar a evitar colisiones excesivas y retransmisiones que desperdician ancho de banda y reducen la tasa de transmisión real. CTS/RTS resuelve esto mediante la introducción de un mecanismo de confirmación (*hand-shaking*) entre los clientes y los AP's. Esta opción es configurable hasta que se logra una tasa de transmisión real óptima.

La falta de cobertura es resuelta mediante la correcta elección de las antenas que se emplearán para los AP. De acuerdo con los datos del fabricante y una serie de pruebas realizadas, es posible obtener la cobertura necesaria para que el desempeño de la red sea el óptimo.

No se considera el problema de los nodos muy próximos así como también el del nodo expuesto, debido a que se empleará un solo AP para cada zona de cobertura. Para el caso de que se requieran más AP's, el problema puede solucionarse mediante el empleo de un canal diferente para cada AP adyacente, tal y como se describe a continuación.

## Planeación de Células

Para una cobertura adecuada en un área plana[6] se recomienda emplear un patrón hexagonal similar al que se utiliza en telefonía celular como se muestra la siguiente figura. Éste patrón ha sido probado durante muchos años y garantiza una cobertura apropiada, baja interferencia y una alta eficiencia en la utilización de ancho de banda con tres canales independientes.

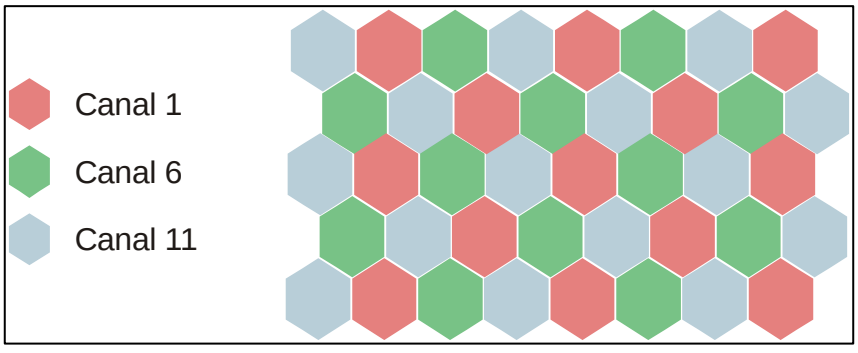



Figura 6.10
*Planeación Celular de Canales no Adyacentes*

[6] En el capítulo 3 se define el concepto de área plana de cobertura

En la figura previa se considera que cada hexágono es el área de cobertura de un punto de acceso trabajando con uno de los 3 canales independientes que son permitidos en las WLAN's (en el caso de que se emplee el estándar 802.11b). Es recomendable que los clientes inalámbricos pertenecientes a cada punto de acceso se ubiquen dentro del hexágono que les corresponde con el objeto de disminuir la posibilidad de problemas de nodos ocultos y nodos expuestos.

***WLAN FI***

La planeación celular debe realizarse cuando se pretende cubrir grandes extensiones y se desea conservar la misma conexión al pasar de una célula a otra (roaming). El diseño que se plantea para la Facultad en las áreas libres no considera esta parte, ya que únicamente se propone una célula por área. En el caso de que posteriormente se requiera extender el rango de cobertura mediante el uso de mas células, bastará con seguir el patrón celular antes mencionado para evitar la interferencia entre dichas células.

### 6.2.5 Verificación de los datos obtenidos

Para finalizar con la sección del diseño de la red, es conveniente emplear una tabla como la que se muestra a continuación, con el objeto de valorar la información que se obtiene a partir de las consideraciones que se han estudiado hasta el momento. Esto nos sirve como referencia para evitar la omisión de puntos importantes en el diseño.

De ésa información es necesario agregar que:

1. Se tienen identificados los Routers y los Switches que pueden servir de soporte para conectar a la WLAN con la red cableada. Sin embargo, por razones de seguridad, no se proporciona el direccionamiento IP ni el nombre oficial de dichos equipos. En caso de que la propuesta sea aprobada, se debe obtener dicha información de manera imprescindible y con la autorización respectiva.

2. Los edificios de la facultad cuentan con más de una planta. Sin embargo, el alcance de esta propuesta no contempla dichas instalaciones. Para una implementación que requiera contemplar varios pisos de un edificio, se deberá instalar al menos un AP para cada uno de ellos, realizando todo el proceso que hasta el momento hemos descrito.

| ACTIVIDAD | INFORMACIÓN A OBTENER |
|---|---|
| **Definición de usuarios** | ▪ Número de usuarios.<br>▪ Aplicaciones a incluir en la red inalámbrica.<br>▪ Especificar tipo de computadora a integrar a la red (Laptop o desktop).<br>▪ Obtener un informe de tráfico estimado. |
| **Definición clara de las zonas de cobertura y sus características** | ▪ Identificar las áreas donde se requiere el servicio.<br>▪ Señalar la ubicación de las zonas de cobertura en un plano de planta a escala. |
| **Verificación de recursos disponibles de los laboratorios de cómputo.** | ▪ Identificar el router de acceso disponible en el edificio, su modelo, puertos libres, dirección IP de loopback y nombre oficial.<br>▪ Identificar si se poseen switches o concentradores en el lugar, su modelo, sus puertos libres, su dirección IP de administración y su nombre oficial. |
| **Verificación de la existencia de fuentes de interferencia dentro del área de cobertura** | ▪ Identificar las posibles fuentes de interferencias como muros de concreto o de superficies metálicas y dispositivos cuya frecuencia de operación sea 2.4GHz.<br>▪ Señalar la ubicación exacta de las fuentes de interferencia en un plano de planta a escala.<br>▪ En caso de que el inmueble cuente con más de una planta y en varios de sus pisos se necesita red inalámbrica, se requiere el plano en elevación para poder identificar la distancia entre pisos. |
| **Estudio de factibilidad para definir los posibles lugares de ubicación de los puntos de acceso** | ▪ En caso de que la propuesta no sea funcional, se procederá a realizar la reubicación del punto de acceso. |

Tabla 6.2
*Tabla de Verificación de los datos obtenidos*

## 6.3 Propuesta de Implementación

### 6.3.1 Estado Actual de la Red Ethernet

En la Facultad de Ingeniería existen dos dependencias que brindan los servicios de apoyo en cómputo dirigidos a los alumnos: la Unidad de Servicios de Cómputo Académico (UNICA) y el Laboratorio de Computación – DIE. El primero de ellos tiene como usuarios a los alumnos de todas las carreras que se imparten en la facultad, mientras que el laboratorio de la DIE está dirigido a los alumnos que cursan las carreras de Ingeniero en Telecomunicaciones, Electrónica o Computación.

También existen otros centros de cómputo, algunos de ellos equipados especialmente para las necesidades de cada carrera, como es el caso del laboratorio de Procesamiento Digital de Imágenes ubicado en el tercer piso del edificio Valdés Vallejo y que está al servicio de los alumnos de la carrera de Ingeniería en Telecomunicaciones. Otro ejemplo (un tanto distinto) es el Laboratorio de Cómputo especializado para la Exploración Petrolera (Schlumberger), que presta sus servicios a los alumnos de las carreras de la División de Ciencias de la Tierra y se encuentra ubicado en el segundo piso del Edificio Principal.

Sin embargo, la propuesta está enfocada a los servicios que prestan los laboratorios de UNICA y la DIE, ya que son éstos quienes cuentan con un mayor número de usuarios, y por otra parte, se encuentran en una ubicación adecuada que facilita la adición de una red WLAN.

Unidad de Servicios de Cómputo Académico UNICA

La Unidad de Servicios de Cómputo Académico (UNICA) "es una dependencia de la Secretaría General de la Facultad de Ingeniería, cuya finalidad principal es la de proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad requiere, recursos de cómputo comerciales y de alta especialización que el avance de la educación, el desarrollo de la informática y el ejercicio profesional demanden".[7]

UNICA cuenta con tres salas de cómputo, dos de ellas ubicadas en el Anexo de la Facultad y uno más en el Edificio Principal.

Es de nuestro interés conocer la infraestructura con la que cuentan estos laboratorios, ya que serán el soporte principal de la red inalámbrica propuesta.

[7] Ésta es la definición que aparece en el sitio WEB dedicado a dicho laboratorio.

## Salas de Cómputo FUNDACIÓN UNAM

Estas salas en conjunto cuentan con 80 servicios disponibles, entendiendo como servicios, el número de computadoras disponibles que cuentan con los servicios de Red e Internet principalmente.

## Laboratorio de Computación DIE

Este laboratorio se encuentra ubicado en el segundo piso del Edificio Valdés Vallejo. Además de brindar el servicio de cómputo a los alumnos, también se desarrollan cursos de manera permanente con el fin de incrementar el conocimiento en el ámbito de la programación y materias relacionadas. Contiguo a este laboratorio de encuentra el laboratorio Microsoft, sustentado por dicha empresa que se encarga de desarrollar nuevos proyectos que involucran por una parte a los estudiantes y por otra a la empresa. Como se mencionó anteriormente, éste laboratorio cuenta con una WLAN en operación.


*Laboratorio de UNICA*

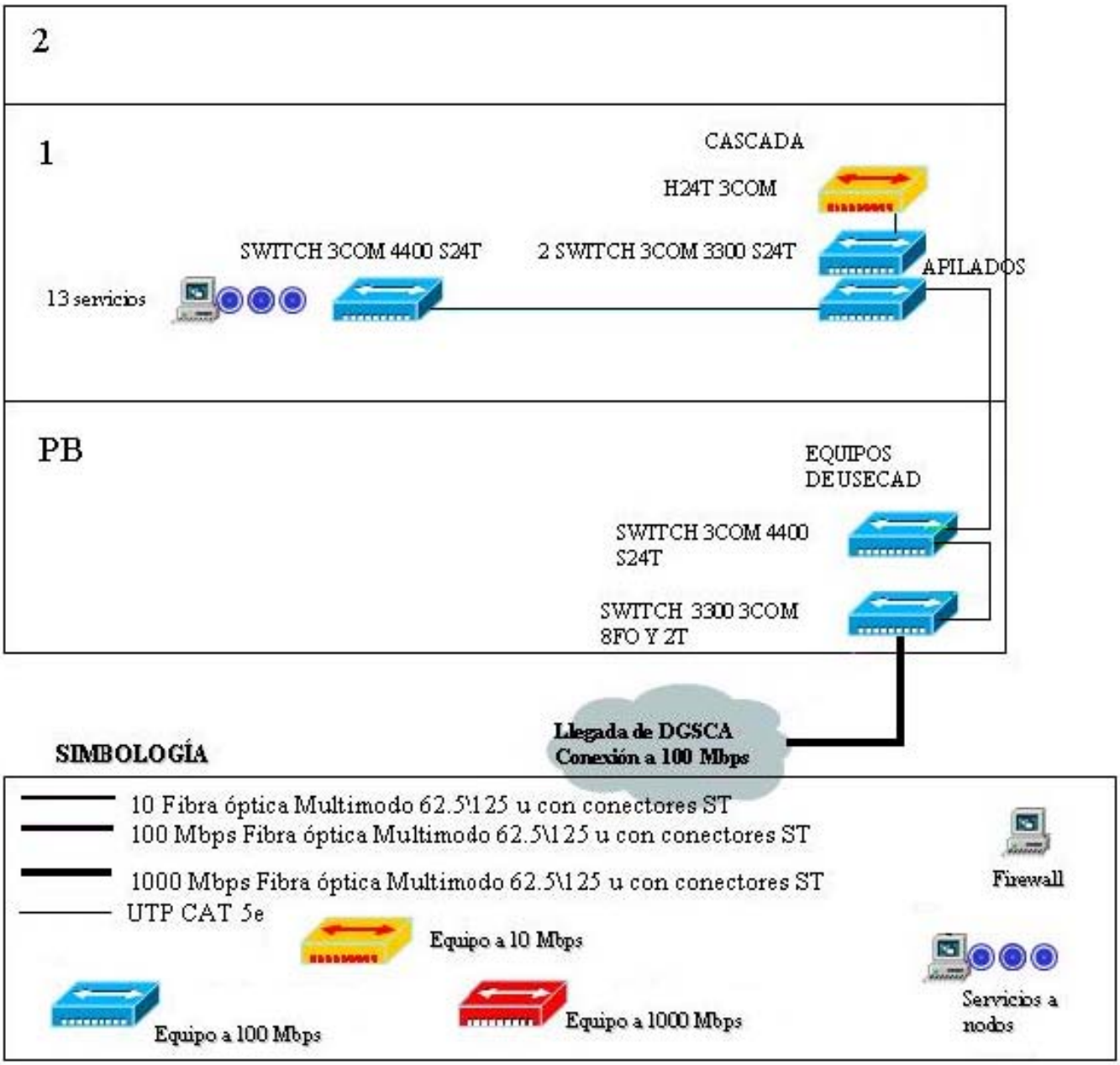

*Laboratorio Fundación UNAM, Planta Baja*


*Laboratorio Fundación UNAM, Planta Alta*

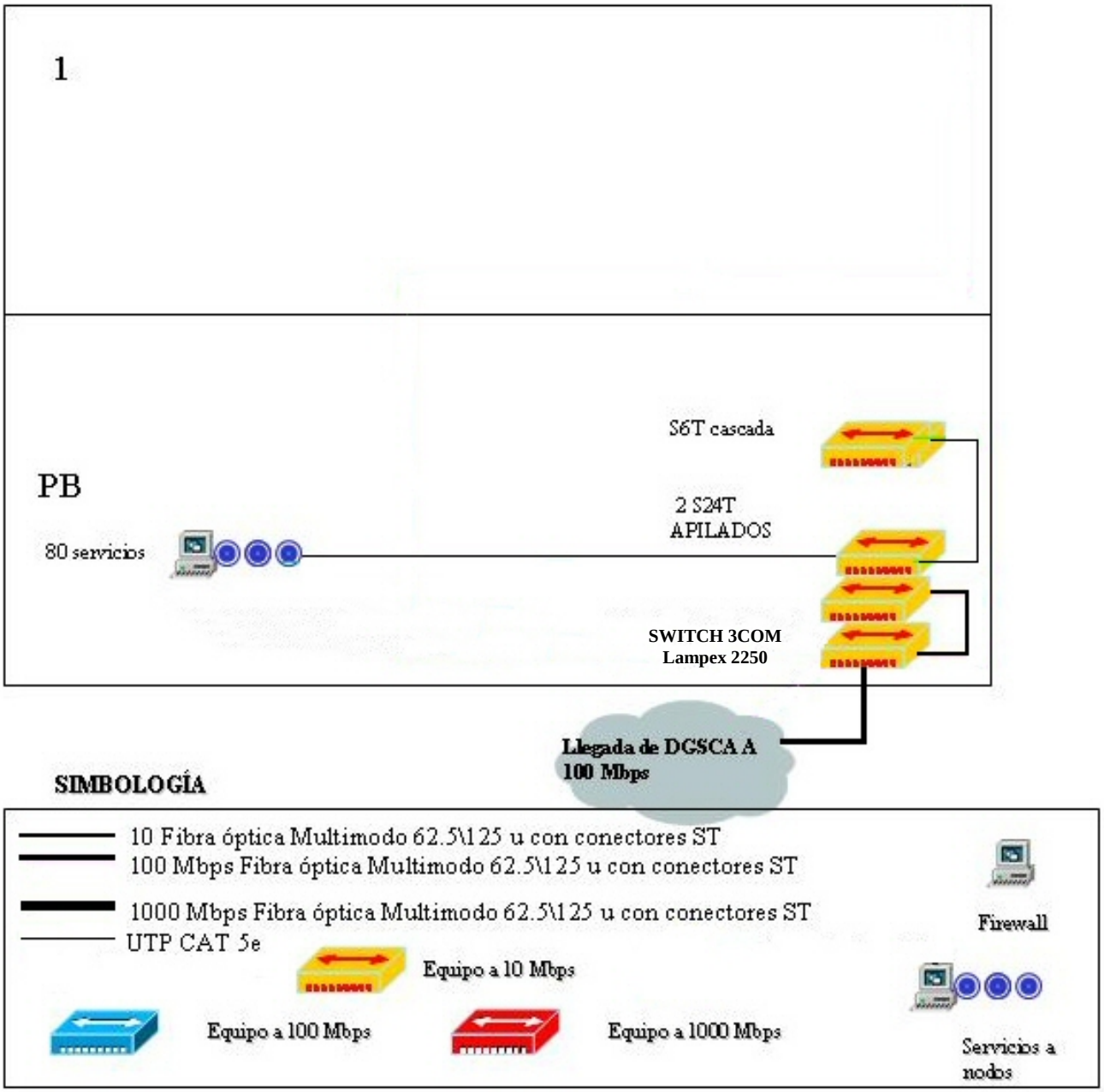
*Laboratorio de Cómputo DIE*

A continuación se presentan los diagramas de la Red actual de éstos centros de cómputo con el propósito de conocer su infraestructura. Cabe señalar que los diagramas se obtuvieron en el mes de Julio del 2004, por lo que están sujetos a cambios sin previo aviso.

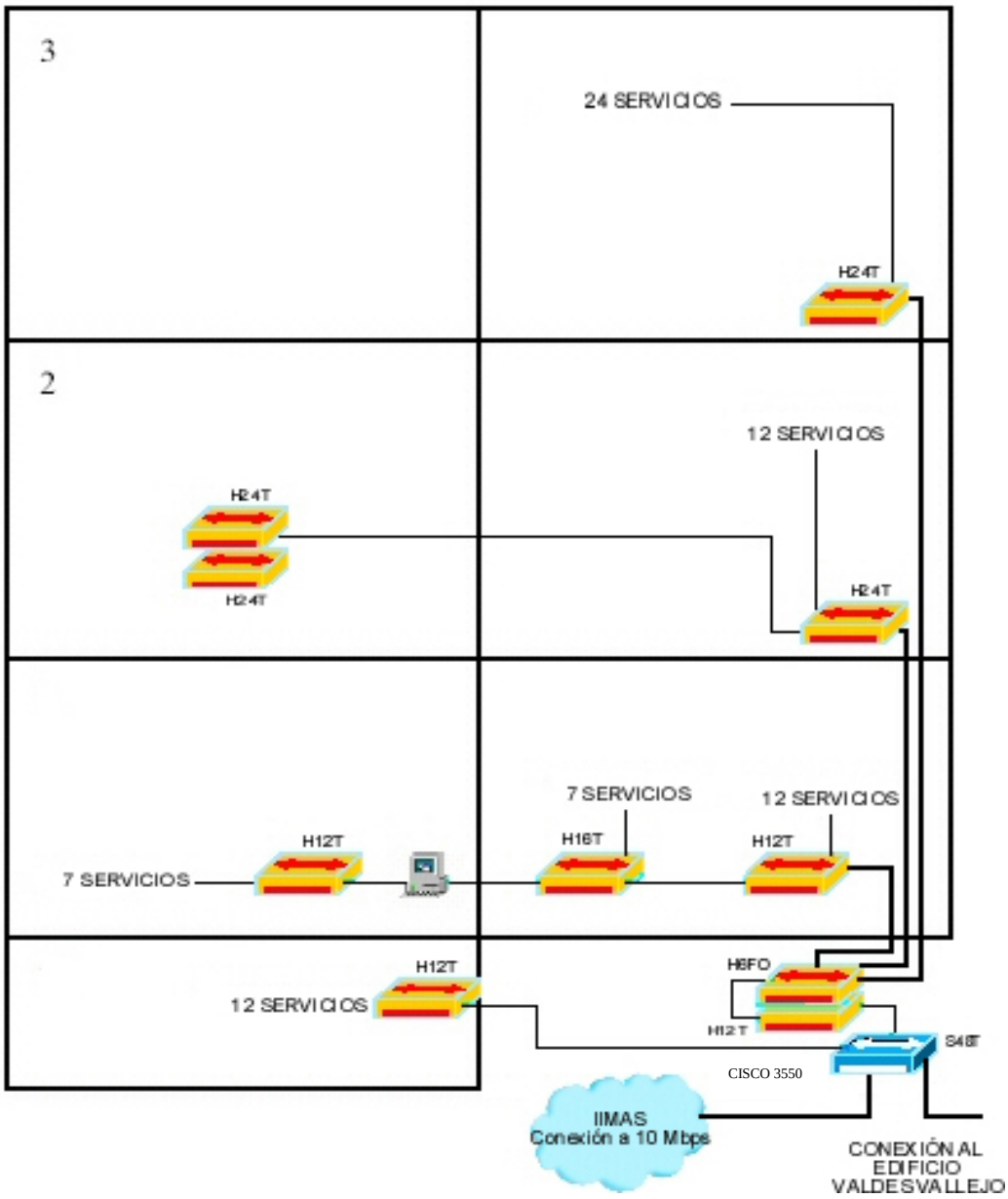
**RED DE CÓMPUTO DE UNICA – SG**
**ZONA A – Edificio Centro de Cálculo**



**RED DE CÓMPUTO DE UNICA – SG**
**ZONA B – Edificio Salas Fundación UNAM**

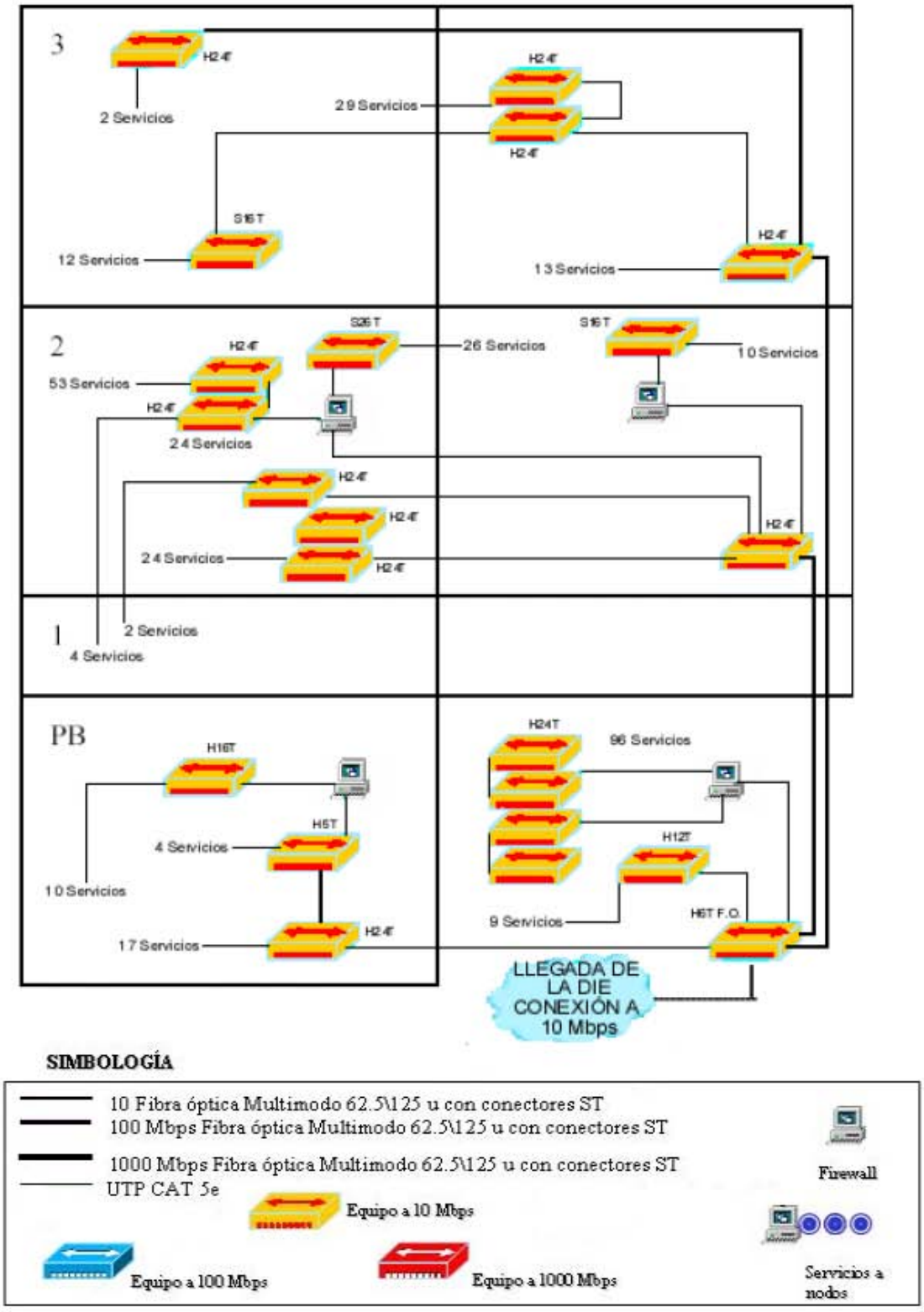


**RED DE CÓMPUTO DIE DIMEI**
**ZONA A – Edificio DIE DIMEI**




**SIMBOLOGÍA**

**RED DE CÓMPUTO DIE DIMEI**
**ZONA B – Luis G. Valdés Vallejo**



### 6.3.2 Requerimientos de Hardware y Software

Para que la WLAN funcione adecuadamente y después de evaluar las condiciones geográficas y las necesidades de los usuarios, se requiere de los elementos que se muestran en el siguiente diagrama (para cada zona de cobertura):

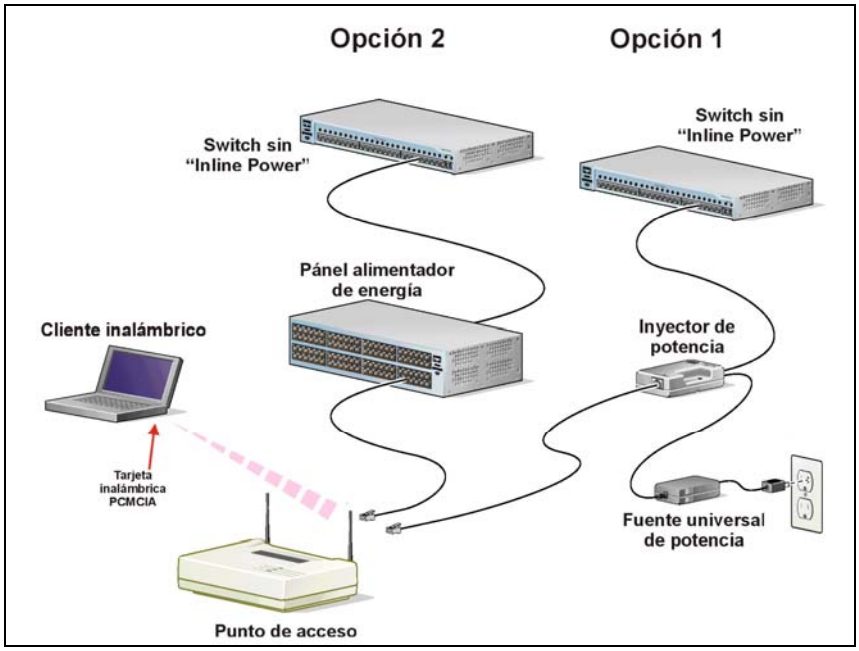



Figura 6.11
*Opciones de Conectividad de Componentes WLAN*

De manera analítica, se necesita:

- Un Punto de Acceso (AP)
- Una antena para el AP
- Cable UTP categoría 5e
- Inyector de Potencia (para la opción 1)
- Fuente universal de potencia (para la opción 1)
- Una Tarjeta Inalámbrica tipo PCMCIA para cada usuario (proporcionada por el mismo)
- Un puerto libre (de un switch o router) 10/100 Base T para la interconexión con la red Ethernet.

La opción 1 debe considerarse cuando el AP se ubicará a una distancia relativamente grande del router/switch que proporcionará el soporte a la WLAN. Para nuestro caso, ésta es la opción correcta.

El Power Inyector (PI) convierte la interfase Ethernet estándar 10/100 Base T (que es más conveniente en interiores) a otra interfase de conector "Tipo F" que emplea cable coaxial y que es más conveniente para ambientes exteriores. Una de las características del PI es que permite que el cableado entre el switch o router y el AP sea de aproximadamente 100 metros, evitando las grandes pérdidas que se obtendrían al emplear un cable UTP convencional. La Fuente Universal de Potencia, consiste en un simple convertidor de corriente alterna a corriente directa (AC-DC).

Los fabricantes de equipo para Redes manejan una tecnología de software para uso exclusivo de sus equipos, es decir, cada marca de router, switch, AP, etc., posee un software en específico para cada producto. Éste software se incluye en conjunto con los productos. Adicionalmente, los fabricantes ofrecen software opcional para incrementar la seguridad y algunas tecnologías que mejoran el desempeño del AP. Por ello, cada AP asegura el correcto funcionamiento del software para el control y administración de los puntos de acceso, así como la interconectividad con la red cableada.

Los sistemas operativos que se deben emplear a nivel usuario son los mismos que utilizan las redes cableadas tradicionales. Esto tiene su justificación en que el modo de operación entre las redes WLAN y las LAN, sólo es diferente en las dos primeras capas del modelo de referencia OSI, y por ende el tráfico de información entre las capas superiores es transparente para la aplicación.

### 6.3.3 Estructura General de la Solución

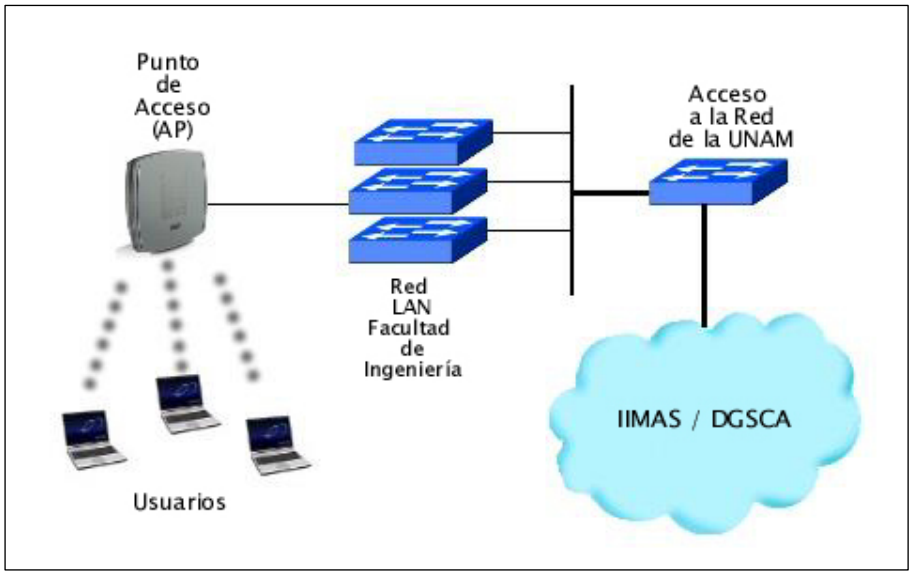



Figura 6.12
*Estructura de la Solución WLAN – F. I.*

La solución propuesta consiste en un diseño centralizado WLAN que permitirá a los alumnos poder tener acceso a los diferentes servicios que los laboratorios de cómputo ofrecen en la actualidad. Para las 3 diferentes zonas de cobertura, la estructura general propuesta es la que se ilustra en la figura 6.12.

### 6.3.4 Solución con Equipo CISCO

El primer elemento a considerar es el AP. Dentro de la gama de Puntos de Acceso CISCO, se propone el AP CISCO Aironet 1300. Las características de este equipo son las siguientes.

El AP Aironet 1300 es un punto de acceso que opera bajo el estándar 802.11g el cual tiene la capacidad de interactuar con dispositivos que manejan el estándar 802.11b. Este AP puede manejar algunas de las opciones avanzadas que encontramos en las redes LAN tradicionales, como son las QoS (calidades de servicio) y las VLAN's. El AP 1300 puede operar como un AP y también puede configurarse como bridge.

Este AP está especialmente diseñado para su empleo idealmente en exteriores, aunque también puede operar en interiores. Una característica muy importante, es que es un producto Wi-Fi certificado, lo cual nos asegura que cualquier dispositivo que cuente con esta certificación, podrá comunicarse con el AP sin importar la marca de dicho dispositivo (obviamente si éste se encuentra dentro de la lista de usuarios de la WLAN y está correctamente configurado). La arquitectura de esta solución se muestra en el siguiente diagrama:

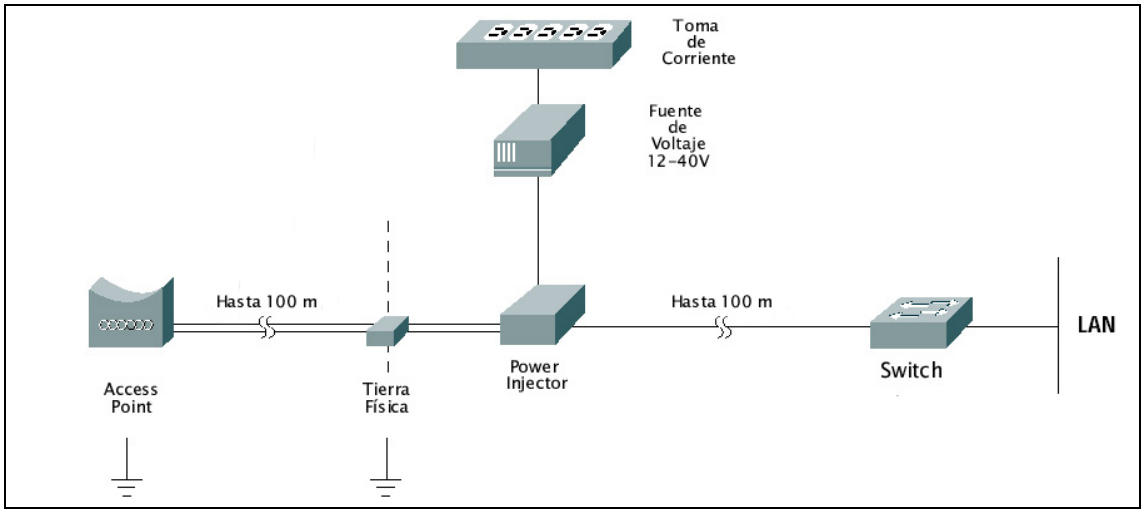



Figura 6.13
*Estructura de la Solución con Equipo CISCO*

A continuación se describe cada uno de los elementos que conforman dicha arquitectura.

## CISCO Aironet 1300

Especificaciones Técnicas

**Número de Parte:** AIR-BR1310G-x-K9-R

Figura 6.14
*Aironet CISCO 1300*

**Compatibilidades:** Compatible con cualquier dispositivo cliente Wi-Fi certificado para capacidades básicas. Compatible con productos CISCO Aironet para capacidades extendidas.

**Protocolos:** Interfase Aérea Estándar IEEE 802.11b, IEEE 802.11g o ambas.

**Banda de: Frecuencias**
2.412 a 2.462 GHz (FCC)
2.412 a 2.472 GHz (ETSI)
2.412 a 2.472 GHz (TELEC)
Para nuestro caso, se deberá emplear la banda de frecuencias 2.412 a 2.462 GHz

**Modulación:**
802.11b - DSSS
• DBPSK a 1 Mbps
• DQPSK a 2 Mbps
• CCK a 5.5 y 11 Mbps
802.11g - OFDM
• BPSK a 6 and 9 Mbps
• QPSK a 12 and 18 Mbps

| | |
|---|---|
| | • 16 - QAM a 24 y 36 Mbps<br>• 64 - QAM a 48 y 54 Mbps |
| **Protocolo de Acceso al Medio:** | CSMA/CA |
| **Canales Disponibles:** | 802.11b/g<br>ETSI: 13<br>América: 11<br>TELEC (Japan): 13<br>Canales sin Sobreposición: 3 |
| **Seguridad:** | Autenticación<br>Soporta 802.1X incluyendo LEAP, PEAP, EAP Message Digest 5 (EAP MD5), EAP TLS, and EAP FAST para entregar autenticación mutual y encriptación dinámica por usuario y por sesión<br>Encriptación<br>Cisco TKIP y WPA TKIP; key handshing (per-packet keying) and MIC listo para AES. |
| **Compatibilidad SNMP:** | Versiones 1 y 2 |
| **Interfaces:** | LEDs de Status: cuatro LEDs: Instalación,<br>Radio, Status y Ethernet bicolor indicando el estado de la fuente de alimentación.<br>Conectores Tipo-F: cable coaxial dual que transporta Ethernet full-dúplex, alimentación DC y el puerto de consola RS-232 full-duplex.<br>Interface para Antenas: Dos conectores tipo RP-TNC para antenas externas. |
| **Desempeño**[7]: | Alcance / Tasa de Transmisión en Exteriores<br>105 metros a 54 Mbps<br>430 metros a 11 Mbps |
| **Potencias de Transmisión Configurables**: | 802.11b<br>100 mW (20 dBm)<br>50 mW (17 dBm)<br>30 mW (15 dBm)<br>20 mW (13 dBm) |

[7] Access Point empleando una antena de 5.2 dBi tipo parche y con clientes que cuentan con equipo CISCO. Los datos mostrados son proporcionados por el fabricante y deben ser empleados únicamente como referencia.

10 mW (10 dBm)
5 mW (7 dBm)
1 mW (0 dBm)

802.11g:

30 mW (15 dBm)
20 mW (13 dBm)
10 mW (10 dBm)
5 mW (7 dBm)
1 mW (0 dBm)

**Sensibilidad de Recepción**: (al 10% con paquetes de 3200 bytes)

1 Mbps: -94 dBm
2 Mbps: -91 dBm
5.5 Mbps: -89 dBm
11 Mbps: -85 dBm
6 Mbps: -90 dBm
9 Mbps: -89 dBm
12 Mbps: -86 dBm
18 Mbps: -84 dBm
24 Mbps: -81 dBm
36 Mbps: -77 dBm
48 Mbps: -73 dBm
54 Mbps: -72 dBm

## CISCO Lightning Arrestor

Protección Contra Descargas (Conexión a Tierra)

Especificaciones Técnicas

**Número de Parte:** AIR-ACC3354

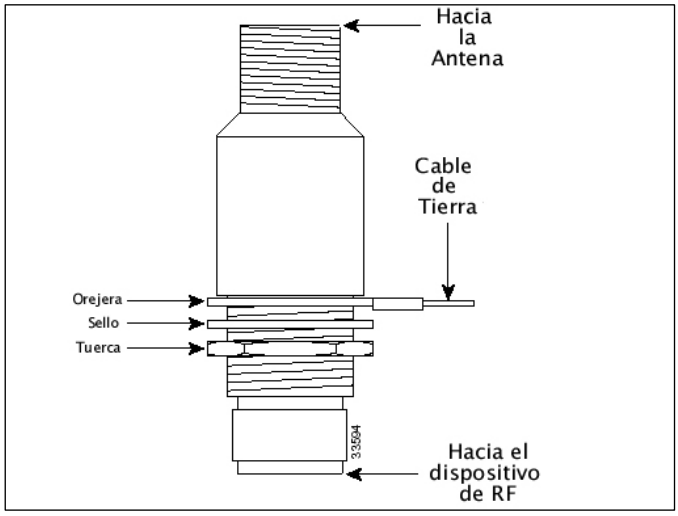



Figura 6.15
*Lightning Arrestor CISCO*

Cuando se instalan antenas en exteriores, siempre existe la posibilidad de que ésta sufra daños debido a descargas eléctricas que se propagan a través de los dispositivos que se encuentran conectados al sistema. Estas descargas pueden ser originadas por relámpagos, o a la estática que produce el viento, por ejemplo. Para solucionar este problema, CISCO cuenta con un dispositivo llamado Lightning Arrestor (LA) diseñado para proteger a los equipos que emplean la frecuencia de 2.4 GHz de la electricidad estática y de las descargas inducidas por diversos fenómenos naturales.

Este dispositivo se instala entre el cable que está conectado directamente a la antena y el dispositivo inalámbrico, en este caso el AP. Pero debido a que emplearemos un Power Injector, el dispositivo de aterrizaje deberá colocarse entre el cable de la antena y el PI. Puede ser instalado en interiores o exteriores, atendiendo las regulaciones locales acerca de las instalaciones eléctricas.

## CISCO Power Injector LR2

Especificaciones Técnicas

**Número de Parte:** AIR-PWRINJ-BLR2

Figura 6.16
*Power Injector CISCO*

| | |
|---|---|
| **Dimensiones:** | 11.73 cm x 12.09 cm x 2.71 cm |
| **Peso:** | 1 kg |
| **Temperatura de Operación:** | -30º a 55ºC |
| **Humedad:** | 0 a 90% @ 38ºC (sin condensación) |
| **Encapsulado:** | Metal |
| **Fuente de Voltaje:** | (proporcionada por el fabricante) |
| **Entrada AC:** | 100 a 240 VAC, +/-10% |
| **Salida DC:** | +48 VDC, +/- 10%, 2 Watts |

**Interfaces:**

LED de Estado: Led bicolor que muestra el estado de la alimentación.

Conectores Tipo-F: cable coaxial dual que transporta Ethernet full-dúplex, alimentación DC y el puerto de consola RS-232 full-duplex

Interfase RJ-45: un puerto de acceso a consola (a 9600 bps) y un segundo puerto para la interfase 10/100 BaseT LAN

Alimentación DC: un conector tipo Switchcraft

## CISCO Antena Omnidireccional 2 dBi Tipo Parche

**Número de Parte:** AIR-ANT5959

Figura 6.17
*Antena Omnidireccional CISCO Tipo Parche*

Esta antena está diseñada para montarse en el techo y su estructura está orientada para su empleo en interiores. A pesar de ello, el sitio donde se planea hacer la instalación de dicha antena, cuenta con la protección suficiente para considerar que no será afectada por la intemperie.

Esta antena opera en la banda de 2.4 a 2.5 GHz y es compatible con los productos CISCO que emplean radio; utiliza conectores tipo RP-TNC (Reverse Polarity-Threaded Naval Connector).

Especificaciones Técnicas

| | |
|---|---|
| **Tipo de Antena:** | Omnidireccional tipo Parche |
| **Frecuencia de Operación:** | 2.4 - 2.5 GHz |
| **VSWR Nominal:** | 1.7:1 |
| **Ganancia Máxima:** | 2 dBi |
| **Polarización:** | Vertical, lineal |
| **Plano Azimuth:** | Omnidireccional |
| **Plano de Elevación 3 dB:** | 70 grados |
| **Dimensiones:** | 13.5 x 7.1 x 2.3 cm |
| **Peso:** | 0.14 kg |
| **Tipo de Conector:** | RP-TNC Macho |
| **Ambiente:** | Interiores, montaje en techo |

Patrón de Radiación en el Plano E

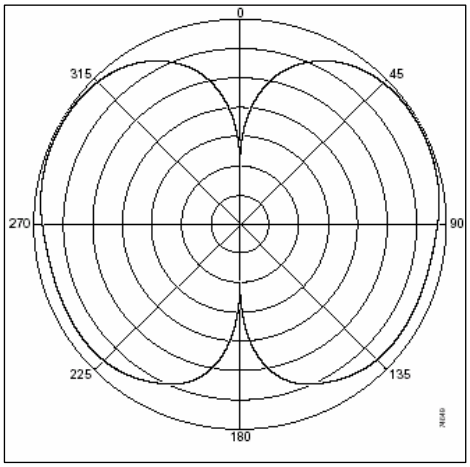



Figura 6.18
*Patrón de Radiación en el Plano H*

Patrón de Radiación en el Plano H

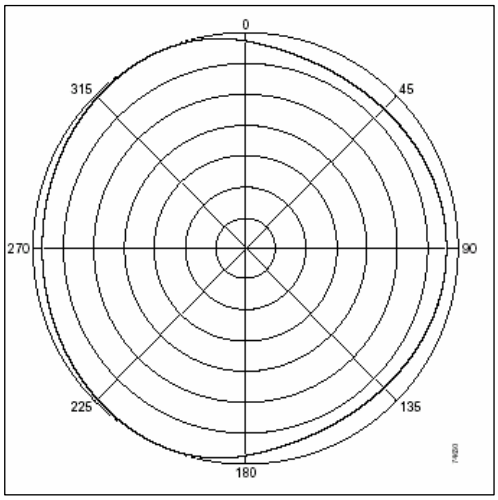



Figura 6.19
*Patrón de Radiación en el Plano E*

Notas Sobre la Instalación

Debido a que las antenas reciben y transmiten señales de radio, éstas son susceptibles a obstrucciones e interferencias propias de los sistemas RF que pueden producir decrementos en la tasa de transmisión real y en el rango efectivo del dispositivo al cual se encuentran conectadas. Para maximizar el desempeño debemos tomar en cuenta lo siguiente:

- Montar la antena para utilizar sus características de propagación. Una forma de lograr esto es orientar la antena lo más horizontal posible, así como a una altura adecuada o bien, lo más cercana al centro del área en la que se requiere cobertura. De esta manera, se maximizan las características de la propagación omnidireccional.
- Mantener a la antena lejos de obstrucciones metálicas tales como instalaciones de calefacción y/o aire acondicionado, estructuras metálicas propias del sitio, cables de alto voltaje, etc.
- La densidad de los materiales empleados en la construcción del edificio determina el número de paredes que la señal puede penetrar para mantener una cobertura adecuada. Los siguientes parámetros pueden emplearse como referencia:

    - El papel y el vinil tienen poca afectación en la penetración de las señales.
    - El concreto sólido y pre-fabricado limita la penetración a una o dos paredes sin degradar la cobertura (dependiendo del ancho de éstas).
    - La señal puede penetrar cinco o seis paredes construidas con tablaroca o madera.
    - Una pared con metal ocasiona que las señales se reflejen, lo que implica una penetración pobre.

Afortunadamente, las áreas de cobertura propuestas no presentan estos problemas de interferencia dado que los únicos obstáculos que se presentan consisten en árboles y algunas columnas pertenecientes a la estructura del edificio.

## CISCO Antena Omnidireccional 5.2 dBi
## Montaje en Mástil

**Número de Parte:** AIR-ANT2506

Figura 6.20
*Antena Omnidireccional CISCO*
*Para montaje en Mástil*

Esta antena está diseñada para las aplicaciones WLAN en la banda de frecuencias de 2.4 - 2.5 GHz, tiene una ganancia nominal de 5.2 dBi y se emplea típicamente en exteriores sobre un mástil. Es compatible con los productos CISCO Aironet que emplean los conectores RP-TNC.

## Especificaciones Técnicas

| | |
|---|---|
| **Tipo de Antena:** | Dipolo |
| **Rango de Operación:** | 2.4 a 2.8 GHz |
| **Para uso en:** | Interiores / Exteriores |
| **VSWR:** | Menor a 2:1. 1:5 nominal |
| **Ganancia:** | 5.2 dBi |
| **Polarización:** | Lineal, vertical |
| **Plano E (3dB):** | Omnidireccional |
| **Plano H (3 dB):** | 40 grados |
| **Longitud del Cable:** | 0.91 m |
| **Dimensiones:** | 29.2 cm x 2.8 cm |
| **Montaje:** | Mástil |

## Patrón de Radiación en el Plano E

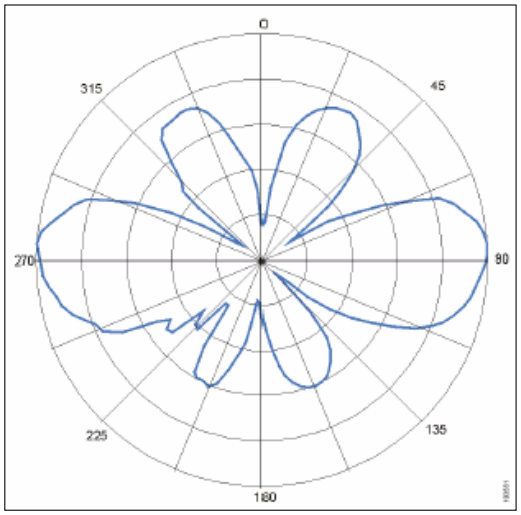



Figura 6.21
*Patrón de Radiación en el Plano E*

## Patrón de Radiación en el Plano H

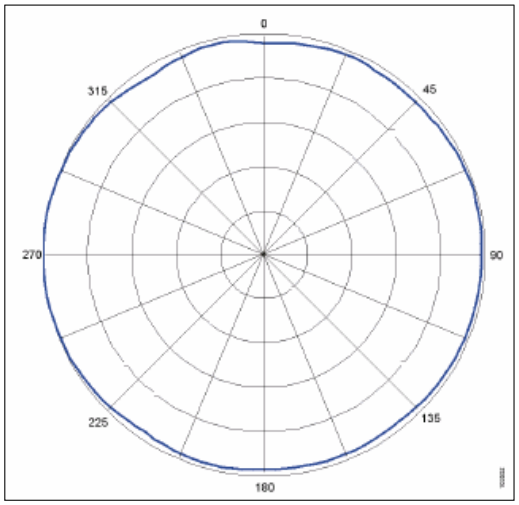



Figura 6.22
*Patrón de Radiación en el Plano H*

## Notas sobre la Instalación de Antenas Montadas en Mástil

- Ensamblar la antena en un sitio que cuente con conexión a tierra física.
- Cuando se coloque la antena en el mástil, se debe estar en contacto con la tierra física.
- Emplear el soporte que se proporciona para ensamblar la antena.
- Se deben tener en cuenta las mismas medidas de seguridad que se emplean en la instalación de una línea de cableado común. Para mayores detalles, consultar el manual de la antena.

## Selección del Sitio

Antes de instalar la antena, se debe pensar cual es el mejor lugar para colocarla con el fin de que se obtenga el mejor desempeño y seguridad.

Generalmente, la instalación de la antena se realiza a una distancia de 1.5 a 3 metros sobre un techo con el objeto de evitar líneas de alta tensión y obstrucciones. De ser posible, se debe encontrar un lugar donde los dispositivos inalámbricos se sitúen por debajo de la antena para que la antena opere con un desempeño óptimo.

En el plano de conjunto (que se detalla al final de este capítulo) muestra cual será la ubicación de las antenas hasta ahora mencionadas. Dicha ubicación obedece a las necesidades de cobertura de las áreas propuestas.

## Cableado

La instalación de las antenas en un sistema inalámbrico debe ser lo más cercano posible a los usuarios. La localización de las antenas no requiere necesariamente estar cerca del site donde se localizan los equipos como el router o el switch. El cable puede tener una longitud de 30 metros o más entre la antena y el AP.

La señal en RF es transportada entre las antenas y el equipo de radio a través de un cable coaxial. Uno de los efectos de emplear un cableado extenso es que se introducen pérdidas en el sistema inalámbrico. Para reducir la atenuación de la señal, se emplearán cables de baja pérdida para conectar estos dispositivos.

El modelo a emplear es el siguiente:

| Modelo | Longitud | Pérdidas |
|---|---|---|
| AIR-CAB020LL-R | 20 ft. (6 m) | 1.3 dB |

Para ejemplificar el efecto que tienen las pérdidas debidas al cable veamos el siguiente ejemplo.

Para un cable de 30 metros, se tiene considerada una pérdida de 6.6 dB, lo que se traduce en un decremento del 30% de la distancia de transmisión. En términos de cobertura, ésta se reduce en un 50% como se muestra en el siguiente diagrama.

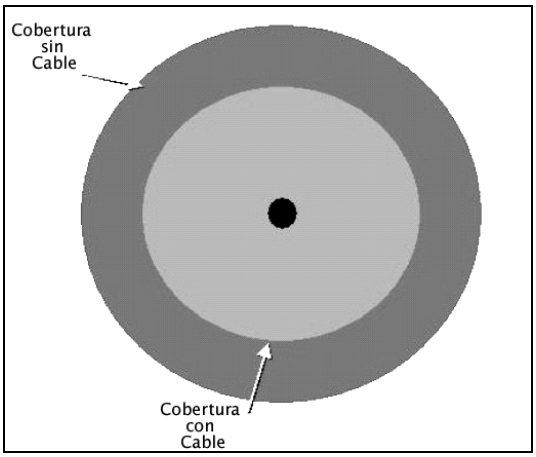



Figura 6.23
*Reducción del Área de Cobertura*

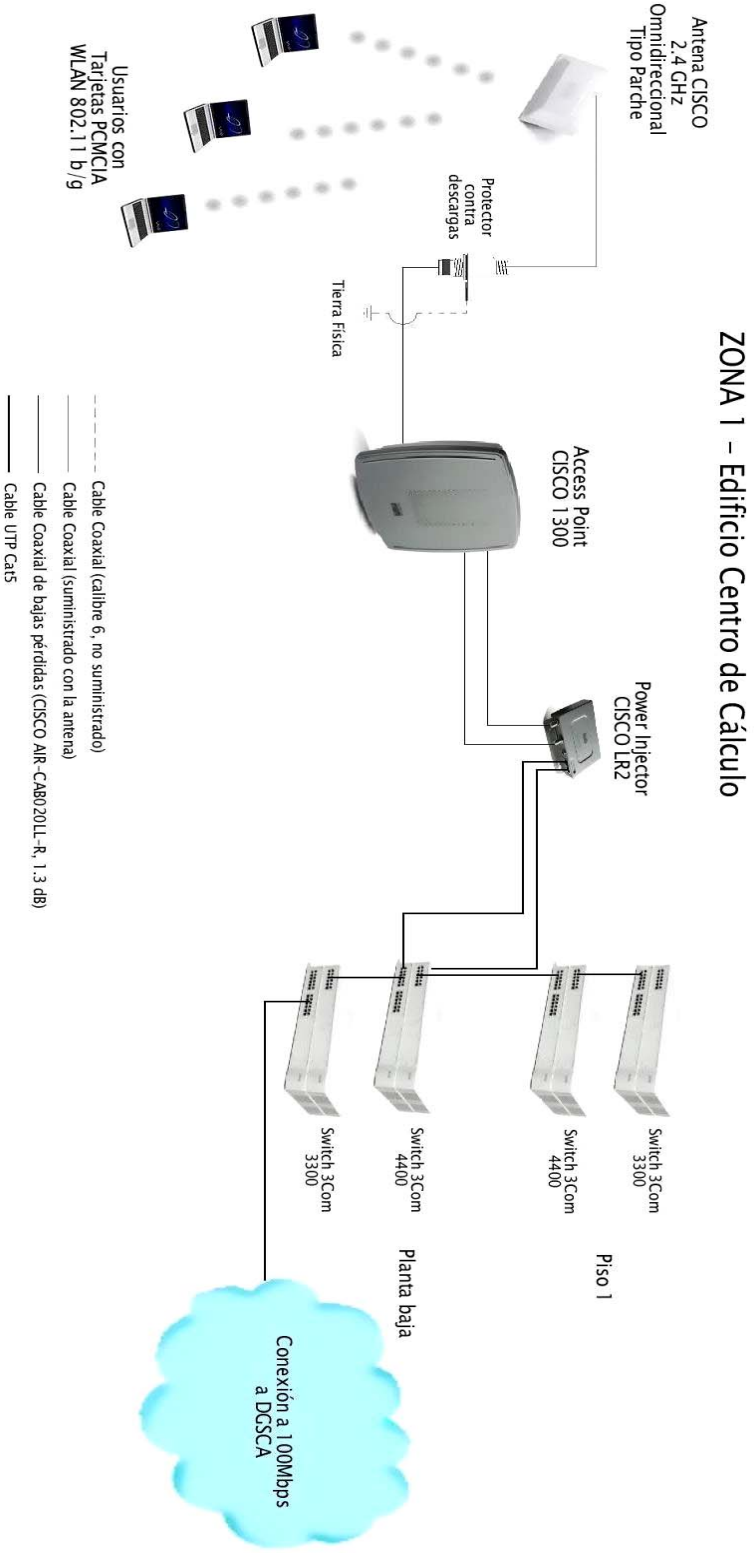
Mientras se esté realizando el cableado, se debe tomar en cuenta lo siguiente:

- Si el cable se coloca muy apretado, puede que las propiedades de atenuación se incrementen. Se debe tratar el cable con mucho cuidado.

- El curveo del cable no debe ser excesivo en los lugares que así lo requieran.
- Se debe cuidar la longitud del cable con el fin de evitar pérdidas excesivas.
- Para las antenas en exteriores, se deben sellar las conexiones que queden expuestas a la intemperie. El uso de silicón puede ayudar a tal propósito.

A continuación se presentan los diagramas de interconectividad con el equipo CISCO propuesto para cada zona de cobertura.

Diagrama de Interconectividad Zona 1 con Equipo CISCO



## Diagrama de Interconectividad Zona 2 con Equipo CISCO

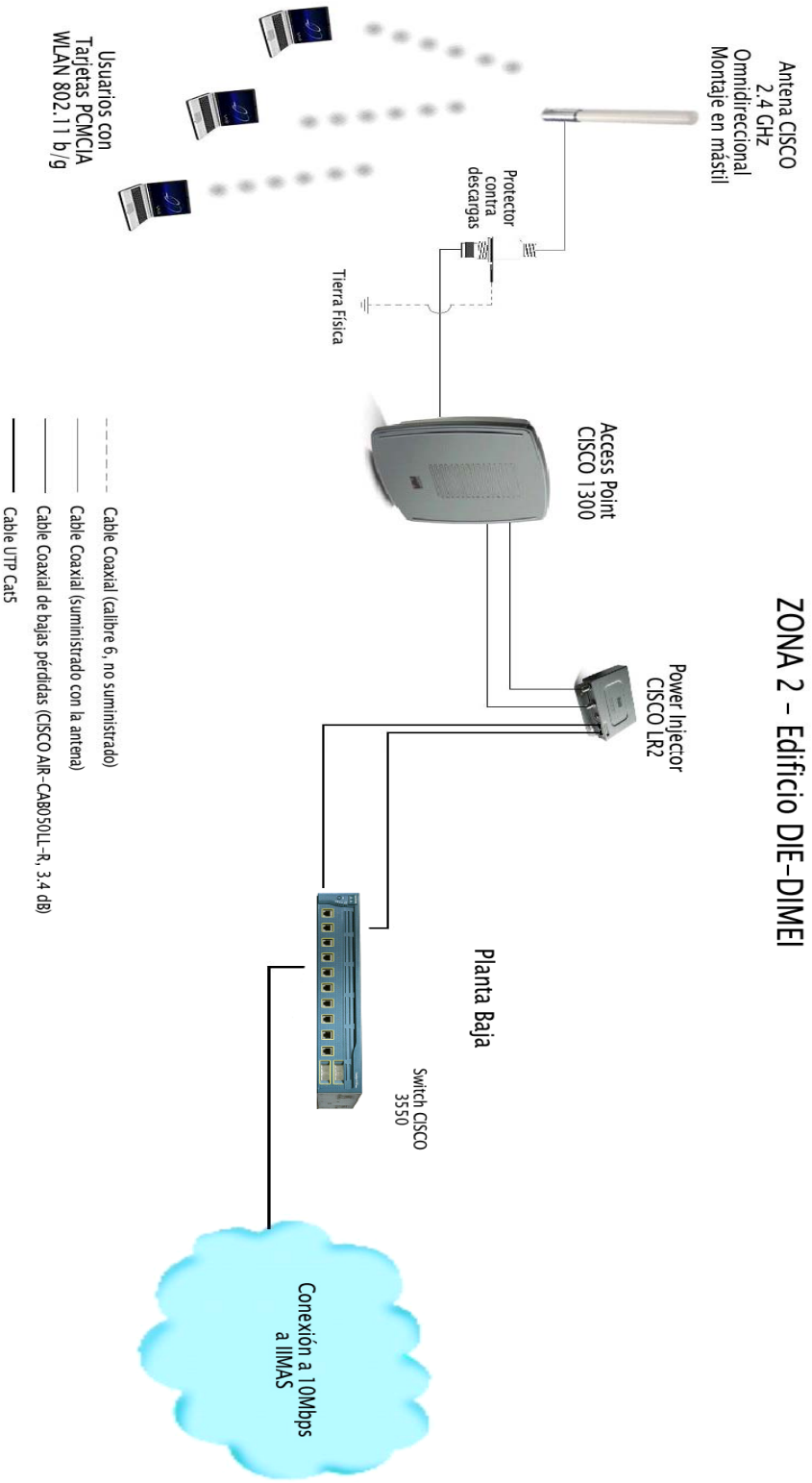
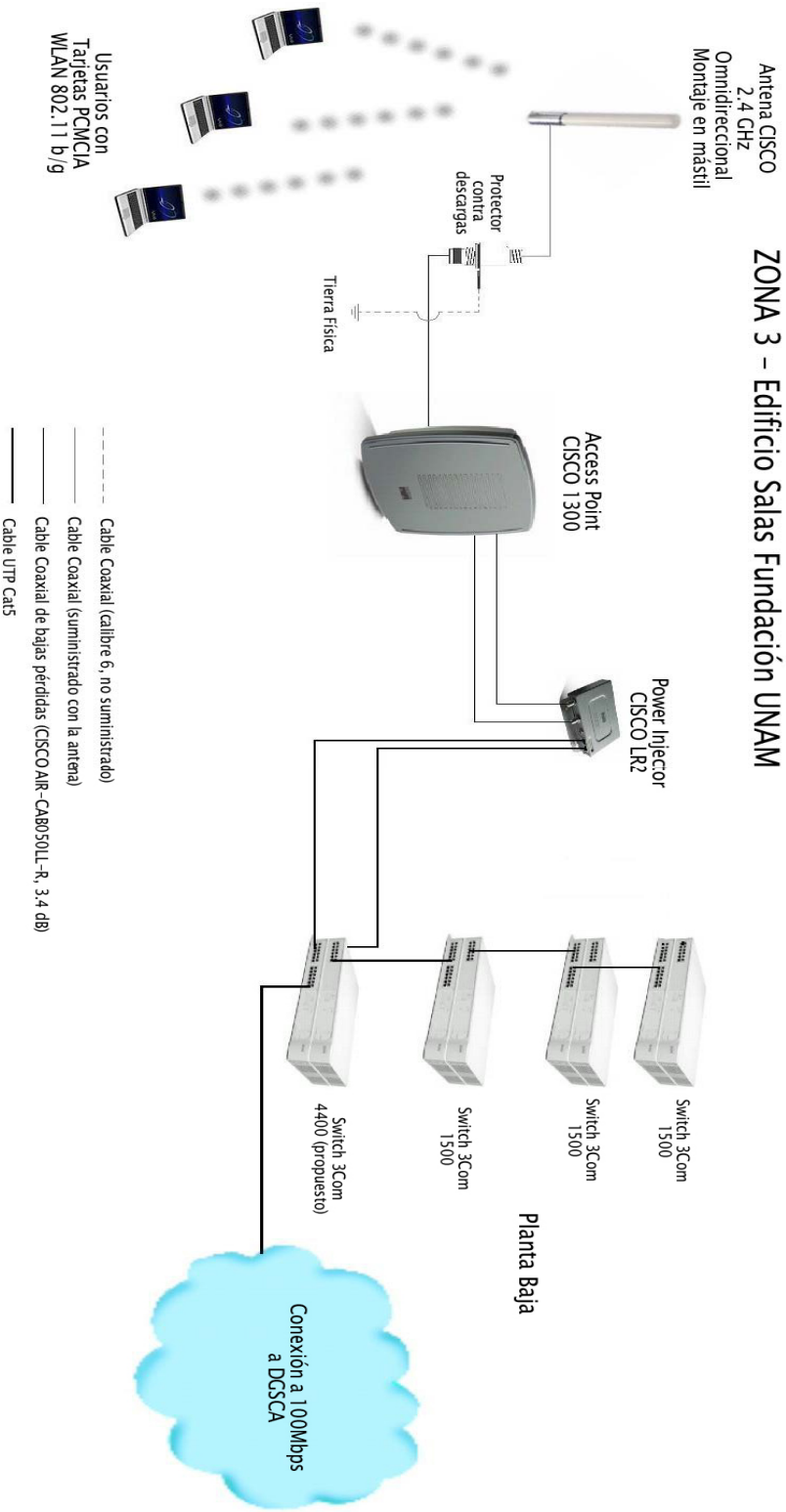


Diagrama de Interconectividad Zona 3 con Equipo CISCO



### 6.3.5 Solución con Equipo 3COM

## 3COM Access Point 8250

Este AP pertenece a la familia de modelos 7250/8250/8500/8750. La diferencia entre ellos radica en el tipo de estándares que pueden operar. El 8250 está equipado de fábrica con una tarjeta para el manejo del estándar 802.11g. Al igual que otros AP's, un hecho que el manejo del estándar 802.11g sea también compatible con el estándar 802.11b, que actualmente es más común encontrarse con este tipo de dispositivos. También cuenta con un slot libre para la adaptación de una tarjeta que soporte el estándar 802.11a.

Figura 6.24
*Access Point 3COM 8250*

Las características de este AP (y por las cuales se propone este modelo) son las siguientes:

Especificaciones Técnicas

**Código** 3CRWE825075A

**Compatibilidades:** Certificación Wi-Fi
WEP, WPA(Wireless Protected Access),
IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
IEEE 802.3af (PoE)

**Administración:** Soporta DHCP, SNMP, autenticación vía RADIUS y administración vía WEB.

**Protocolos:** Modulación
802.11a: OFDM,
802.11g: OFDM and DSSS (con codificación Barker y CCK para asegurar la compatibilidad con 802.11b)

**Canales de Disponibles:** 802.11a: 36-64 (8 en total sin sobreposición),
802.11g: 1-11 (América)

**Seguridad:**

Autenticación

Acceso Remoto vía RADIUS basada en direcciones MAC. WPA, autenticación TKIP mediante los protocolos EAP-MD5, EAP-TLS, EAP-TTLS y PEAP.

Encriptación

Encriptación avanzada mediante WPA de 256 bits, 40/60 bits, 128 y 154 bits. Llave compartida mediante WEP. Encriptación DSL (Dynamic Security Link), propietaria de 3Com.

**Control de Acceso:** Filtrado de direcciones MAC mediante listas de control.

**Desempeño:**

Rango de Operación (interiores)

802.11a: hasta 50 metros de transmisión recepción

802.11g: hasta 100 metros de transmisión recepción

**Potencias de Transmisión:**

802.11g: 17dBm dependiendo de la tasa de transmisión

**Sensibilidad de Recepción:**

802.11a

6 Mbps: - 84 dBm, +/- 2 dBm (dependiendo de la banda)
12 Mbps: - 82 dBm
36 Mbps: - 73 dBm
54 Mbps: - 66 dBm

802.11g

1 Mbps: - 96 dBm
2 Mbps: - 94 dBm
5.5 Mbps: - 92dBm
11 Mbps: - 88 dBm
12 Mbps: - 86dBm
24 Mbps: - 85 dBm
36 Mbps: - 80dBm
54 Mbps: - 73 dBm

## 3COM Antena Omnidireccional 2.5 dBi Tipo Parche

Esta antena expande el rango de transmisiones de datos vía inalámbrica, proporcionando a sus usuarios inalámbricos acceso en movimiento. Soporta los puntos de acceso AP 3Com Wireless LAN Access Point 7250, 8250 y 8750.

Figura 6.25
*Antena Omnidireccional 3COM 2.5 dBi*

La antena omnidireccional proporciona cobertura uniforme en todas direcciones en grandes áreas abiertas. Está diseñada para su instalación en interiores. A pesar de ello, el sitio exacto donde se planea realizar la instalación de esta antena no está afectada por la intemperie, por lo que se considera que el lugar seleccionado es apropiado para colocarla.

Especificaciones Técnicas

| | |
|---|---|
| **Código:** | 3CWE492 |
| **Frecuencia de Operación:** | 2300 – 2500 Mhz |
| **Ganancia:** | 2.5 dBi |
| **Polarización:** | Vertical, lineal |
| **Conector:** | Tipo N |
| **Banda VSWR:** | <1.35:1 |
| **Potencia Radiada Efectiva (ERP):** | Alta: 112 mW; Media: 36 mW; Baja: 9 mW |
| **Temperatura De operación:** | - 40º C a 80º C |

Patrón de Radiación en el Plano E

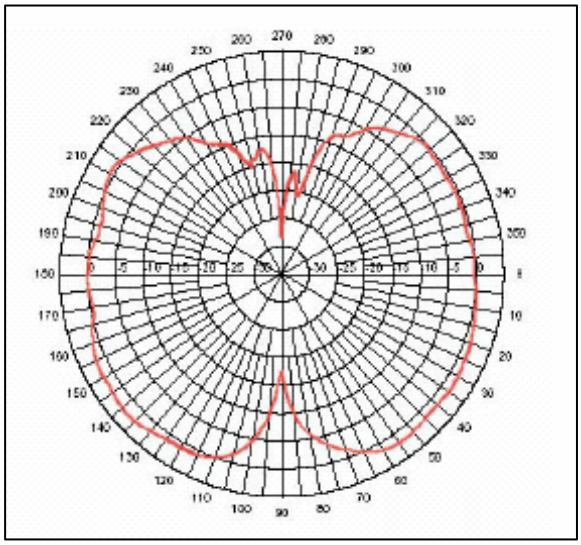


Figura 6.26
*Patrón de Radiación en el Plano E*

Patrón de Radiación en el Plano H

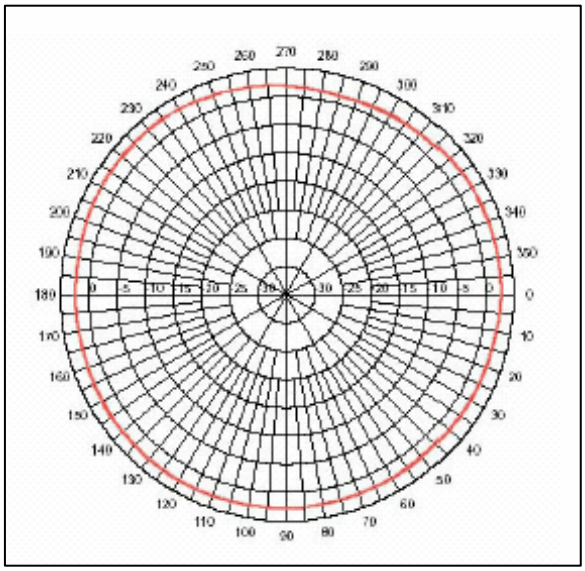


Figura 6.27
*Patrón de Radiación en el Plano H*

## 3COM Antena Omnidireccional 4 dBi Tipo Parche

Figura 6.28
*Antena Omnidireccional 3COM 4 dBi*

Esta antena expande el rango de transmisiones de datos vía inalámbrica, proporcionando a sus usuarios inalámbricos acceso en movimiento. Soporta los 3Com Wireless Access Point 7250, 8250 y 8750 para proporcionar una cobertura uniforme en una amplia área interior o exterior.

La antena omnidireccional de fibra de vidrio está diseñada para utilizarse en entornos tanto interiores como exteriores

Especificaciones Técnicas

**Código** 3CWE490

**Frecuencia de Operación:** 2.400 - 2.4835 GHz

| | |
|---|---|
| **Ganancia:** | 4 dBi |
| **Banda VSWR:** | <1.5:1 |
| **Potencia Radiada Efectiva (ERP):** | Alta: 159 mW; Media: 50 mW; Baja: 13 mW |
| **Temperatura de Op.:** | - 40º C a 80º C |
| **Polarización:** | Vertical |
| **Resistencia al viento:** | 125 mph |
| **Peso:** | 166 gramos |

Patrón de Radiación en el Plano E

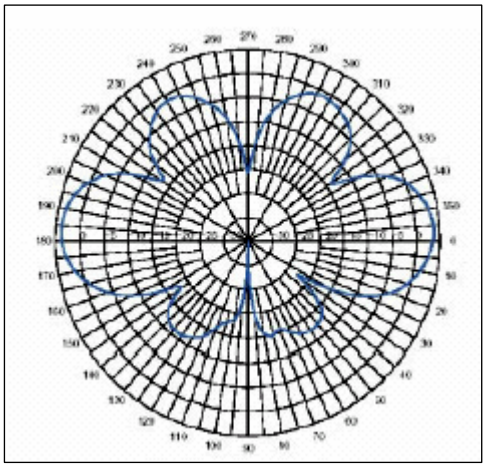


Figura 6.29
*Patrón de Radiación en el Plano E*

Cableado

Figura 6.30
*Cable de 1.8 m 3COM*

Se empleará el cable 3Com de 1.8 metros para la interconexión de la antena con al AP.

Especificaciones Técnicas

| | |
|---|---|
| **Código:** | 3CWE580 |
| **Conectores:** | Tipo N a SMA |
| **Pérdidas:** | 2 dBi @ 2.4 Ghz<br>4 dBi @ 5 Ghz |
| **Longitud:** | 1.8 metros (6 Ft) |

A continuación se presentan los diagramas de conectividad con los equipos propuestos.

Diagrama de Interconectividad Zona 1 con Equipo 3Com

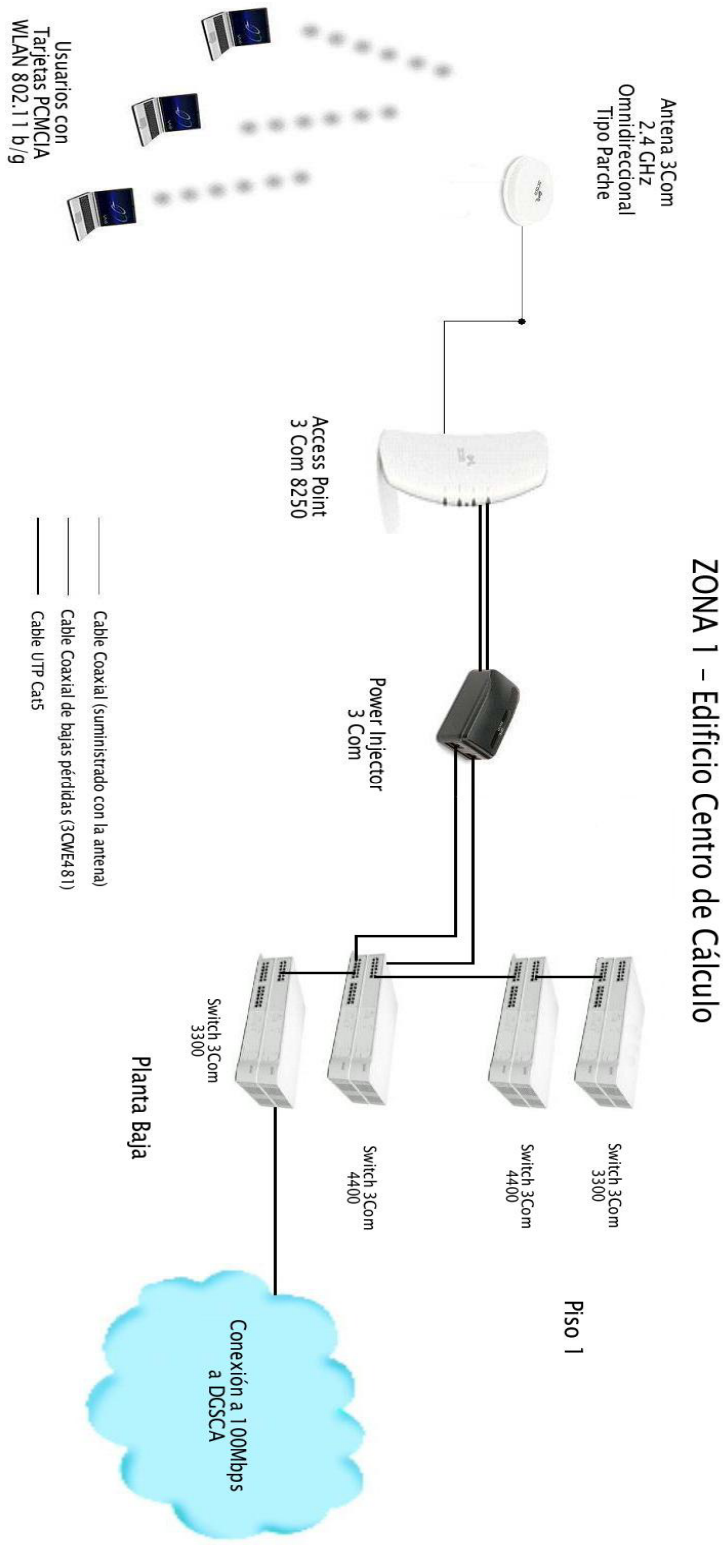


Diagrama de Interconectividad Zona 2 con Equipo 3Com

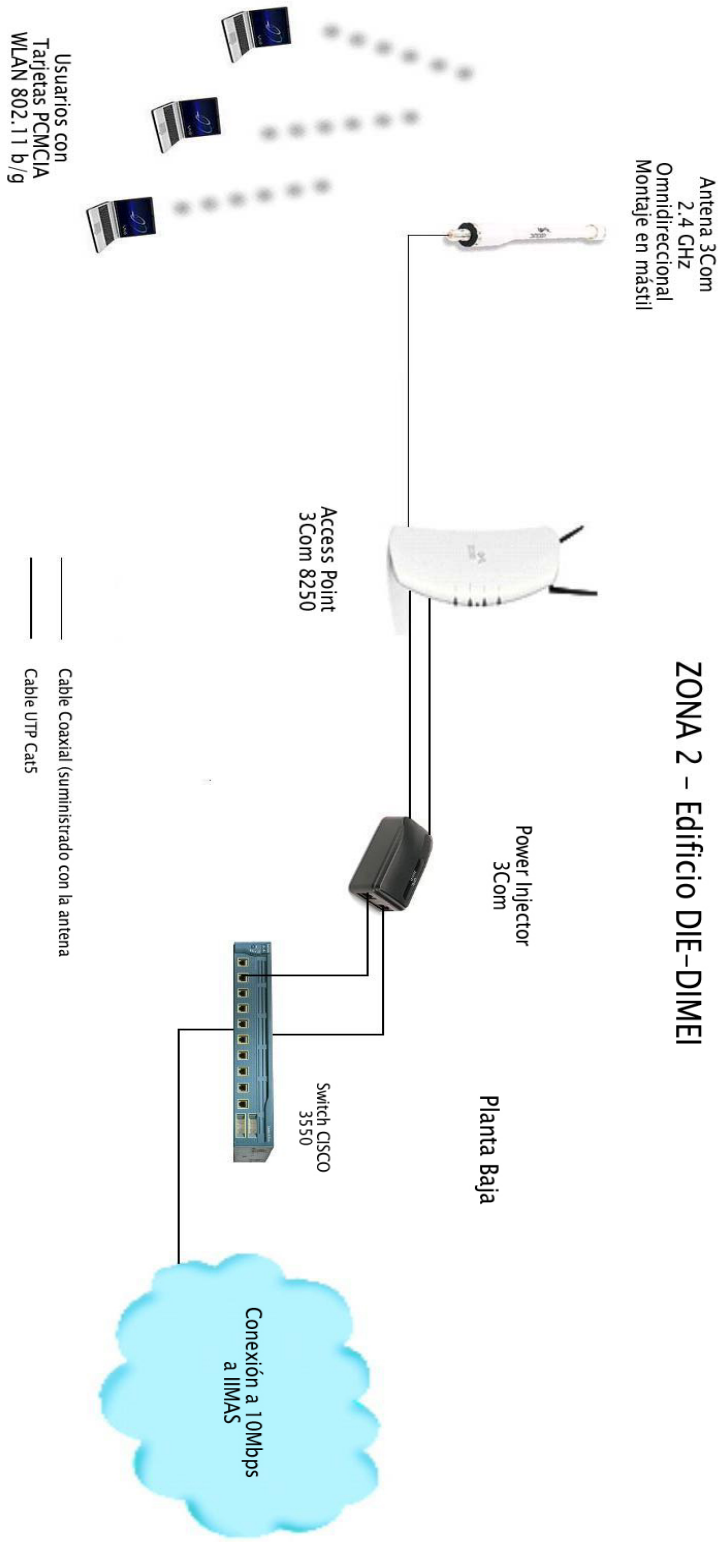
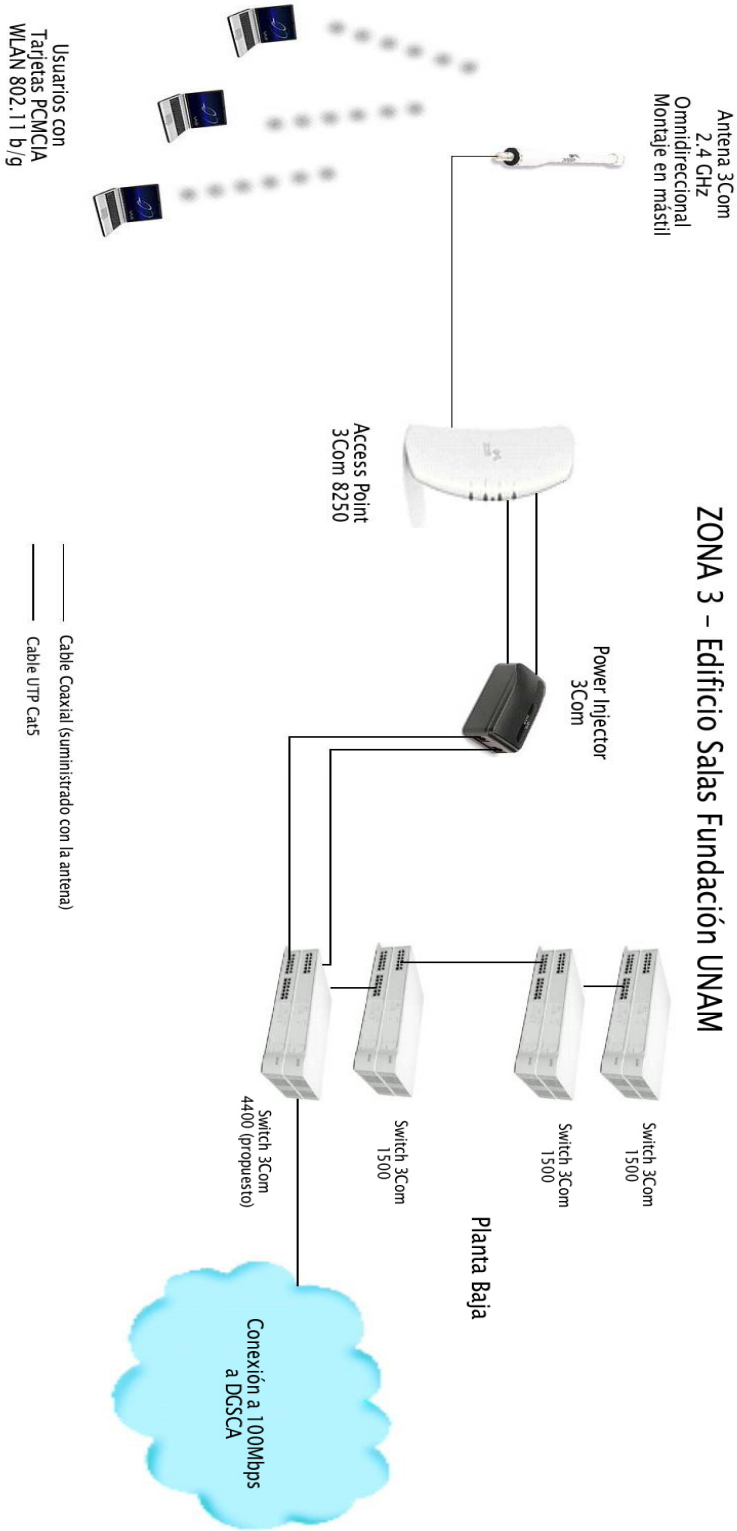


Diagrama de Interconectividad Zona 3 con Equipo 3Com



### 6.3.6 Interconexión con la Red LAN

Hasta el momento hemos analizado los factores que intervienen en el diseño de la futura red WLAN. Pero una parte fundamental consiste en el análisis para la interconexión de los equipos que forman parte de la red actual y la WLAN propuesta. De hecho, de eso depende que el desempeño de la red inalámbrica pueda tener los resultados esperados.

La interconexión de una red LAN con una WLAN puede hacerse a través de dos dispositivos: los switches y los routers. Los laboratorios de cómputo cuentan con switches para recibir los enlaces de datos que tienen su origen en el IIMAS y DGSCA y en específico, emplean los siguientes equipos:

Switch 3COM 4400
Switch 3COM 3300
Switch 3COM 2550
Switch CISCO 3550

A continuación se describen las características de cada equipo (sólo las esenciales), con el objeto de analizar las capacidades de cada uno, así como la compatibilidad con los equipos WLAN.

**Switch 3COM 4400**

| | |
|---|---|
| **Puertos:** | 24 o 48 puertos autonegociables 100BASE-TX<br>1 puerto de consola RS232 |
| **Seguridad:** | Autenticación vía Servidor RADIUS (IEEE 802.1x)<br>Contabilidad de Sesiones<br>Secure Shell (SSHv2)<br>IEEE 802.1x Autenticación de usuarios |
| **Desempeño:** | Opera en Capa 2 y 4<br>(modelo de 24 puertos)<br>8.8 Gbps de velocidad de retransmisión<br>6.6 millones de paquetes por segundo<br>8 000 direcciones MAC soportadas<br>64 VLAN's (802.1Q)<br>IGMP v1 y v2<br>Soporta DHCP |
| **Estándares SNMP:** | SNMP v1 |
| **Spanning Tree:** | IEEE 802.1D Protocolo Spanning Tree (STP)<br>IEEE 802.1w Protocolo Rapid Spanning Tree (RSTP) |

## Switch 3COM 3300

| | |
|---|---|
| **Puertos:** | 24 Puertos 10/100 autonegociables<br>1 puerto de consola RS-232 |
| **Seguridad:** | Contabilidad de Sesiones<br>Secure Shell (SSHv2)<br>IEEE 802.1x Autenticación de usuarios |
| **Desempeño:** | Estándar IEEE 802.1Q<br>IGMP v1 y v2<br>Soporta DHCP |
| **Estándares SNMP:** | SNMP v1 |
| **Spanning Tree:** | IEEE 802.1D Protocolo Spanning Tree (STP)<br>IEEE 802.1w Protocolo Rapid Spanning Tree (RSTP) |

## Switch 3COM 2250

| | |
|---|---|
| **Puertos:** | 48 puertos 10 / 100 |
| **Estándares:** | ISO 8802-3<br>IEEE 802.3 (Ethernet)<br>IEEE 802.3u (Fast Ethernet)<br>IEEE 802.1d (bridging)<br>IEEE 802.3x (flow control)<br>IEEE 802.3ab (Gigabit Ethernet)<br>IEEE 802.1p (traffic prioritization) |
| **Desempeño:** | Soporta hasta 8000 direcciones MAC |

**Nota:** A comparación de los switches 3COM de modelos superiores, las capacidades de éste Switch resultan bastante reducidas, por lo que no sería conveniente interconectar la WLAN concretamente por lo siguiente: no soporta mecanismos de seguridad que serán indispensables en la operación de la WLAN. Tampoco soporta el estándar 802.1Q referente al manejo de VPN's, lo cual podría afectar de manera significativa el desempeño de la WLAN.

Por lo anterior, se recomienda la implementación de un nuevo Switch con las capacidades del 3COM 3300 como mínimo.

## Switch CISCO 3550

| | |
|---|---|
| **Puertos:** | 10BASE-T RJ-45; Categoría 3, 4, o 5 UTP<br>100BASE-TX RJ-45 Categoría 5 UTP<br>Puerto de consola RJ-45 |
| **Seguridad:** | Autenticación RADIUS, SSH, Kerberos, TACACS y SNMP |
| **Desempeño:** | 8.8 Gbps de velocidad como mínimo para la retransmisión de paquetes<br>Soporta un mínimo de 8000 direcciones MAC<br>Soporta QoS<br>Soporta IGMP<br>Soporta VLAN Trunking (VTP) |
| **Estándares de Capa 2:** | Direccionamiento IP a través de RIP v1 y V2, OSPF, IGRP, EIGRP, BGPv4 |
| **Estándares:** | IEEE 802.1x<br>IEEE 802.1w<br>IEEE 802.1s (Multiple Spanning Tree Protocol, MSTP)<br>IEEE 802.3x full duplex en puertos 10BASE-T, 100BASE-TX, y 1000BASE-T<br>IEEE 802.1D Spanning-Tree Protocol<br>IEEE 802.1Q VLAN's<br>Estándares RMON I y II<br>SNMPv1, SNMPv2, SNMPv3 |

De acuerdo a lo expuesto en las secciones anteriores, podemos afirmar que la interconexión entre un AP y un switch es semejante a una configuración típica de una red LAN entre un switch y un hub. Con base en ello se tienen las siguientes consideraciones:

1. Si el switch tiene puertos de 10/100 Mbps, quiere decir que cualquier dispositivo que se conecte a uno de ésos puertos también contará con la misma velocidad de transmisión. Es decir, el AP conectado a un puerto 10/100 tendrá en teoría el mismo ancho de banda que el switch.
2. La velocidad de transmisión puede ser determinada a través de la configuración manual o automática del switch (en el caso de switches con puertos autonegociables). Ésta decisión debe ser tomada por el administrador de red.
3. Para segmentar el tráfico de la red así como a los dominios de colisión, es recomendable la configuración de VLAN's. Los switches anteriormente analizados tienen esta capacidad (a excepción del switch 3COM 2250). Para

resolver ésta último problema, se propone la sustitución de este switch por otro de mayores capacidades, que es el CISCO 4400.

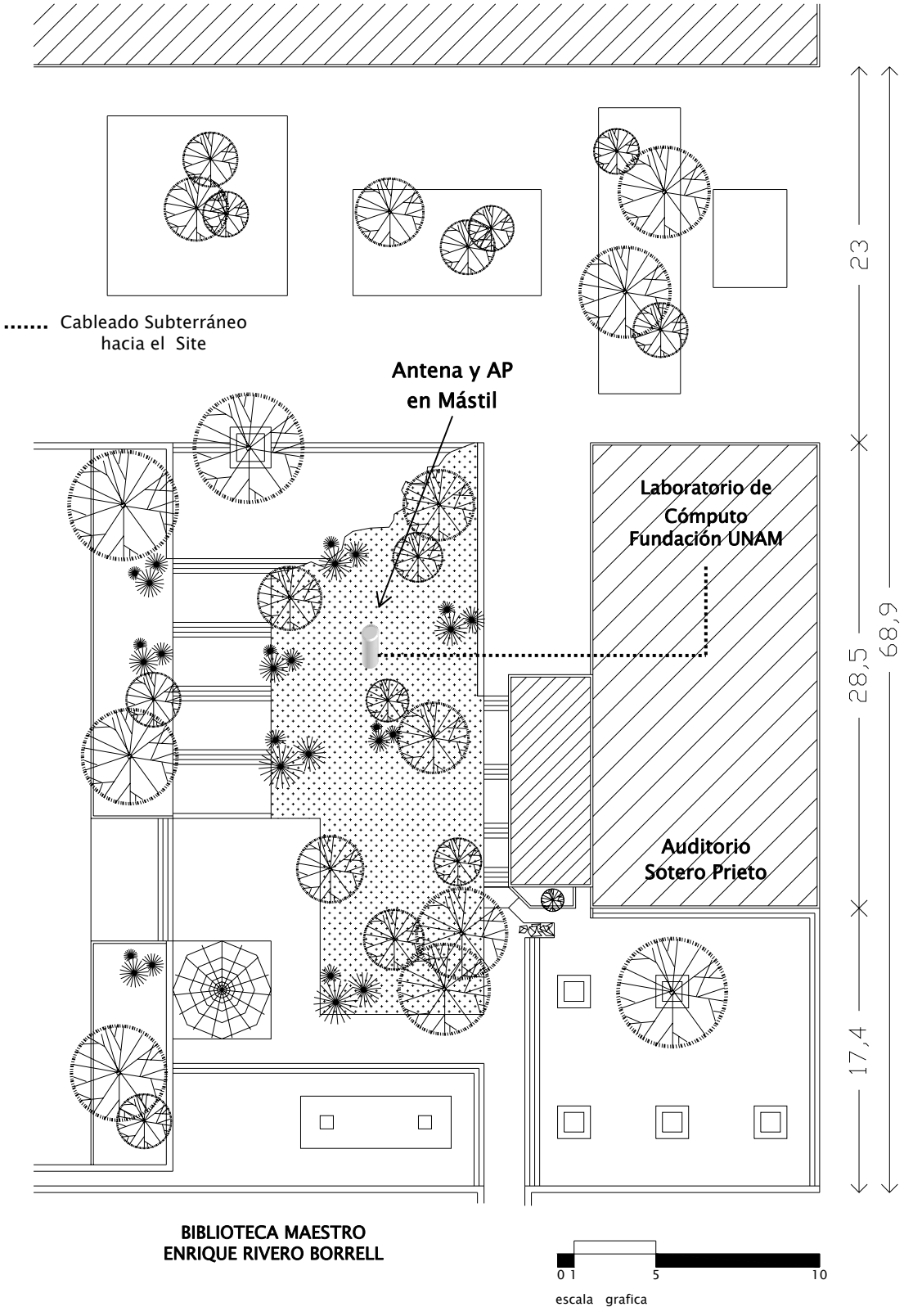
Por todo lo anterior, no se encuentra inconveniente alguno para la interconexión de la red WLAN propuesta con la red LAN actual.

### 6.3.7 Ubicación de los AP's y Cobertura Esperada

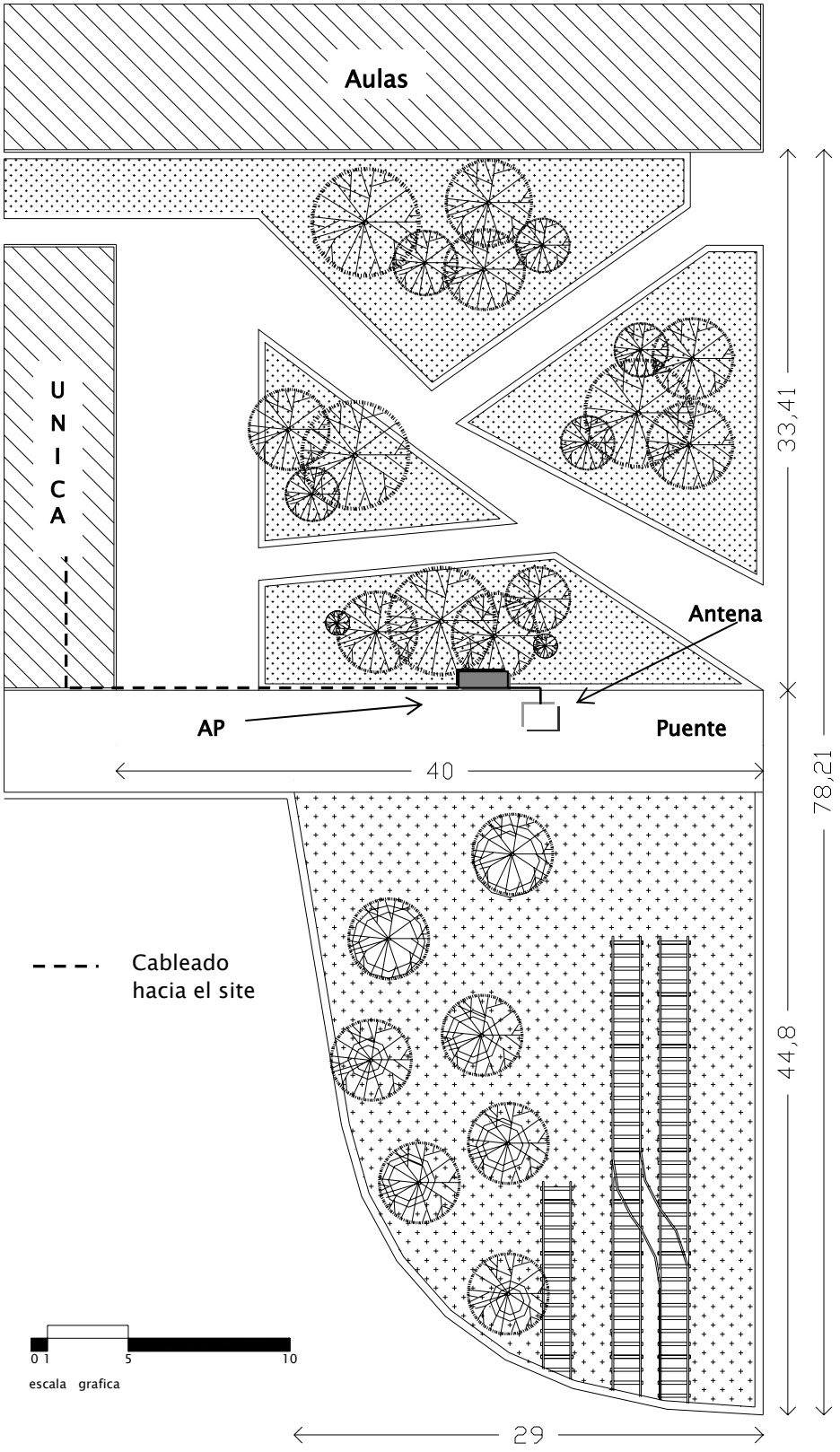
La ubicación de los AP's y de las antenas posee gran relevancia para obtener la cobertura necesaria de acuerdo a cada zona propuesta. Dicha ubicación de los AP´s y sus respectivas antenas se eligió en la parte más céntrica de las áreas de cobertura con el fin de aprovechar las características de transmisión de las antenas (ya que transmiten en forma omnidireccional). Además, con el uso de los Power Injector es posible interconectar los AP's con la red LAN sin rebasar el límite de distancia entre estos dispositivos, la cual es de 100 m.

A continuación se presenta en las siguientes plantas de conjunto, las ubicaciones precisas de los AP y sus antenas.

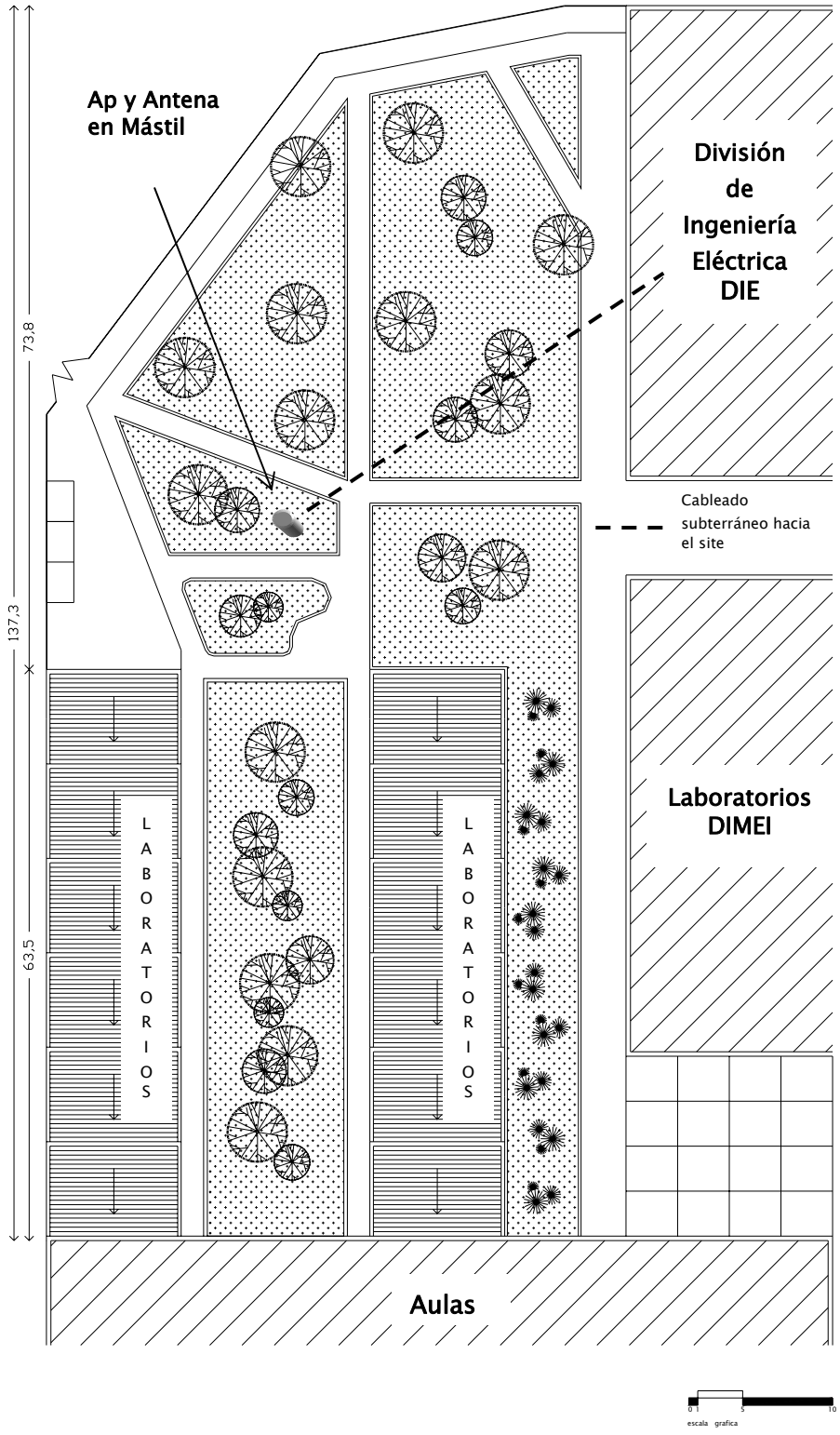
## Planta de Conjunto Zona 1



Planta de Conjunto Zona 2



## Planta de Conjunto Zona 3



### 6.3.8 Desempeño Esperado de la Red

Se han estudiado las principales características de las áreas de propagación de la señal, así como los equipos propuestos para la implementación de la WLAN. En este breve apartado, se habla del desempeño de la red que se espera, en términos de ganancia (potencia) de transmisión.

De manera general, se plantea que dicho desempeño depende de los siguientes factores:

- Equipo de Transmisión
- Medio de Propagación
- Equipo de Recepción

El análisis de pérdidas y ganancias en los elementos citados, se resume de la siguiente manera:

- Potencia efectiva de transmisión: Potencia de Transmisión [dBm] – Pérdidas en el cable de conexión [dB] + Ganancia de la Antena [dBi]
- Pérdidas de Propagación [dB]: Pérdidas en Espacio Libre [dBi]
- Sensibilidad Efectiva del Receptor [dBi]: Ganancia de la antena [dBi] – Pérdidas en el cable de conexión [dB] – Sensibilidad del Receptor [dBm]

Para un desempeño aceptable de la WLAN, la potencia de transmisión + las pérdidas de propagación + la sensibilidad del receptor deben ser mayores que cero. El residuo brinda el margen del sistema. Un buen enlace WLAN tiene como margen un valor de 6 a 10 dB.

Las propiedades de transmisión y recepción no siempre son idénticas en ambos sentidos, por lo que se recomienda realizar un cálculo en ambas direcciones, es decir, en la dirección AP – Cliente y Cliente - AP.

Análisis del Enlace con Equipo CISCO

**(AP – Cliente)**

| | | |
|---|---|---|
| Potencia de Transmisión[a]: | 20 | dBm |
| Perdidas del Cable Tx: | 1.3 | dB |
| Ganancia de la Antena Tx[b]: | 2 | dBi |
| Pérdidas en el Espacio Libre[c]: | -76 | dB |
| Ganancia de la Antena Receptora[d]: | 0 | dBi |

| | | |
|---|---|---|
| Pérdidas del Cable Rx[e]: | 0 | dB |
| Sensibilidad Efectiva Rx[f]: | -67.6 | dBm |

**Margen Total: 12.3 dB**

**(Cliente – AP )**

| | | |
|---|---|---|
| Potencia de Transmisión[g]: | 17 | dBm |
| Perdidas del Cable Tx[e]: | 0 | dB |
| Ganancia de la Antena Tx[d]: | 0 | dBi |
| Pérdidas en el Espacio Libre[c]: | -76 | dB |
| Ganancia de la Antena Receptora[b]: | 2 | dBi |
| Pérdidas del Cable Rx: | 1.3 | dB |
| Sensibilidad Efectiva Rx[h]: | -72 | dBm |

**Margen Total: 16.3 dB**

**Consideraciones:**

a. La potencia de transmisión corresponde al máximo permisible que equivale a 100 mW.

b. La ganancia de la antena corresponde al modelo de montaje en techo. La antena montada en mástil tiene una ganancia mayor, igual a 5.2 dBi

c. Las pérdidas en el espacio libre se calculan de acuerdo a la fórmula P(dB)= 92,45 + 20log10 F+20 LOG10d. Donde: P = pérdidas [dB]; F = Frecuencia [GHz] y d = distancia en kilómetros [km]. Para obtener el valor de -76 dB, se consideró una distancia máxima de 60 metros alrededor de la antena transmisora.

d. Debido a que el fabricante no proporciona un valor determinado de la ganancia de la antena, se considera el valor de 0 dB.

e. Como la antena está integrada dentro de la tarjeta adaptadora PCI, se considera que no hay pérdidas significativas entre la antena y el módulo receptor.

f. La sensibilidad efectiva es dependiente de la tasa de transmisión. Se está considerando un valor de - 67.6 dBm (la cual es la más baja) que corresponde

a la tasa de transmisión a 54 Mbps en el modelo 3CRWE154G72 del fabricante 3Com. En este caso no se sugiere una tarjeta CISCO, ya que su precio es considerablemente mayor respecto de otros fabricantes y el presupuesto de los clientes (de la red) resulta ser muy variado.

g. Se emplea el mismo modelo de tarjeta PCI que el inciso anterior f.

h. Valor correspondiente a una tasa de transmisión de 54 Mbps. A tasas menores aumenta este valor.

Análisis del Enlace con Equipo 3Com

**(AP – Cliente)**

| | | |
|---|---|---|
| Potencia de Transmisión[a]: | 17 | dBm |
| Perdidas del Cable: | 2 | dB |
| Ganancia de la Antena[b]: | 2.5 | dBi |
| Pérdidas en el Espacio Libre[c]: | -76 | dB |
| Ganancia de la Antena Receptora[d]: | 0 | dBi |
| Pérdidas del Cable[e]: | 0 | dB |
| Sensibilidad Efectiva[f]: | -67.6 | dBm |

**Margen Total: 9.01 dB**

**(Cliente –AP)**

| | | |
|---|---|---|
| Potencia de Transmisión: | 17 | dBm |
| Perdidas del Cable Tx: | 0 | dB |
| Ganancia de la Antena: | 0 | dBi |
| Pérdidas en el Espacio Libre: | -76 | dB |
| Ganancia de la Antena Receptora: | 2.5 | dBi |
| Pérdidas del Cable: | 2 | dB |
| Sensibilidad Efectiva: | -66 | dBm |

**Margen Total: 7.5 dB**

**Consideraciones:**

Aplican las mismas que se mencionan al emplear equipo CISCO, obviamente con los valores proporcionados por el fabricante 3Com.

Existen más factores que afectan de manera directa el desempeño de la red, y algunos de ellos se han mencionado en las secciones anteriores: la zona de fresnel, la difracción y las multitrayectorias.

En los dos primeros casos, no existe problema alguno ya que dichos factores afectan principalmente a radio enlaces punto a punto; además, en nuestro sistema, se espera que los usuarios tengan línea de vista directa entre dispositivos, eliminando así los problemas de difracción.

El caso de las multitrayectorias si es competencia de nuestro sistema. El receptor recibirá la señal que está siendo propagada por el AP, pero también recibe las señales que provienen de los objetos que están reflejando la misma señal y con un ligero retraso. Esto provoca la cancelación de la señal en algunos casos, y también provoca que se reciban diferentes señales en el dominio del tiempo. En general esto se traduce en errores en la transmisión.

La manera de reducir estos efectos se encuentra dentro de los algoritmos de modulación (en el caso de OFDM por ejemplo) y diversas técnicas empleadas por los fabricantes. La forma de medir el impacto de las multitrayectorias se hace a través del BER (Bit Error Rate) que ofrece cada fabricante y sujeto a los límites que marca el Estándar 802.11. Otra forma de evitar las multitrayectorias es tener línea de vista directa entre el transmisor y receptor, que para nuestro caso, ocurrirá en la mayoría de los casos.

# Conclusiones

Las redes inalámbricas (WLAN) están conformadas por un conjunto de dispositivos electrónicos que son capaces de intercambiar información de manera inalámbrica; en otras palabras, el tráfico de datos se realiza a través de ondas radioeléctricas. Se originan a partir de nuevas necesidades demandadas por los usuarios de las Redes LAN, entre las cuales la más importante es la movilidad, ya que las características propias dichos sistemas, han podido satisfacer con un desempeño óptimo altas tasas de transmisión, confiabilidad en los enlaces y seguridad en el transporte de la información. La tendencia de las WLAN's apunta a la posible oferta de que éstas puedan ofrecer las mismas características con las que actualmente cuentan las Redes LAN.

Actualmente se requiere que ambos tipos de redes tengan un punto en común, es decir, que se encuentren interconectadas. Por ello no podemos decir que hoy día una tecnología sea la sustitución de la otra, y por el contrario ambas se visualizan como complementarias.

En 1997 se formula el Estándar IEEE 802.11, el cual emite una serie de recomendaciones para lograr que los equipos de los diversos fabricantes sean interoperables. Después de ello, las investigaciones continúan, dando lugar a la mejora significativa del desempeño de las WLAN's y en la creación de nuevos estándares para el aumento de las tasas de transmisión y de la seguridad principalmente.

Como la industria implementa de forma casi inmediata los últimos avances tecnológicos, resulta cada vez más atractivo el empleo de la tecnología WLAN. Por esta razón, diariamente se incrementa el número de usuarios que deciden utilizar una WLAN. Esto también tiene su efecto en la reducción de los costos de los equipos y de su implementación. Basta recordar que a mayor consumo, menor costo.

Todos estos factores impulsaron la idea de formular un proyecto en donde los estudiantes pudieran tener acceso a esta nueva tecnología. En otras universidades como el Tecnológico de Monterrey y la Universidad Anáhuac, por ejemplo, ya se encuentran sistemas de este tipo; de ahí que se considera que es el momento oportuno de que nuestra Universidad sea partícipe de los avances más recientes en lo que a éste rubro se refiere.

Existen algunos laboratorios WLAN en nuestra Facultad, pero no hay algún proyecto que esté diseñado para los espacios abiertos, tal y como se formula en el presente trabajo. En la delimitación del tema se tomaron en consideración las recomendaciones emitidas por los jefes de las unidades de cómputo académico, pues no se trataba de crear un proyecto que fuera desarrollado de manera simultánea por las distintas entidades. Como resultado, fueron elegidas las áreas libres con las que cuenta la Facultad de Ingeniería.

Pero el reto no fue sencillo. En primer lugar, resultó complicado encontrar bibliografía suficiente que abarque todos los temas que conciernen a las WLAN's, situación por la cual se recurrió a la búsqueda en Internet de los artículos más recientes acerca de la nueva tecnología. Cabe señalar, que se encontró en menor medida documentos técnicos elaborados en nuestro idioma. Para evitar este problema en lo posterior, ésta tesis contempla también como objetivo, brindar de manera sintética los conocimientos técnicos básicos acerca de la composición y operación de los sistemas WLAN.

La elección de un sistema WLAN depende de las necesidades de cada organización. En el análisis de dichas necesidades, se encontró que resulta viable implementar una red WLAN para nuestra Facultad porque cada vez es más grande el número de usuarios que tienen la posibilidad de emplear ésta tecnología. Si bien el número de alumnos no se verá incrementado próximamente, el empleo de una WLAN permitirá descentralizar los servicios de cómputo académico, cuyo efecto está en una mejor distribución de las instalaciones destinadas para tal fin.

En los sitios donde se propone instalar la WLAN no se presentan problemas de consideración en cuanto a cobertura y propagación, ya que el equipo de la propuesta cumple con los requisitos mínimos necesarios para superar los obstáculos que se pudieran presentar. De manera específica, se trata de áreas al aire libre, donde los factores de atenuación e interferencia son casi inexistentes (a causa de la absorción de la señal por edificios y objetos).

El problema que tal vez podría causar impactos importantes en el desempeño de la Red, es el de las multitrayectorias, debidas a reflexiones en tierra y a diversos obstáculos en los alrededores (arboles, jardineras, bancas, personas, etc). Sin embargo, se analizó que los métodos de modulación en espectro disperso ayudan a contrarrestar los efectos antes mencionados.

Una parte que deberá cuidarse en el momento de la implementación es el resguardo de los equipos, pues al estar expuestos al aire libre, pueden ser objeto del vandalismo. En el mercado existen diversos productos que ayudarán a evitar ese tipo de situaciones. Aunado a esto, sería positivo sensibilizar a los usuarios para que ellos mismos sean partícipes en el cuidado de los equipos.

Los equipos propuestos para la implementación, cumplen de manera teórica el objetivo principal. Las marcas utilizadas para la propuesta fueron seleccionadas debido a que tienen la mayor presencia en el mercado. Se recomienda ampliamente la solución CISCO, debido a que éste fabricante ofrece información más completa acerca de las características de los equipos y mayor soporte (tanto a nivel personal como en Internet); aunado a esto, se puede apreciar mayor robustez en la operación, por el hecho de contar con mecanismos de seguridad desarrollados por la compañía. La solución 3Com ofrece una instalación más sencilla y de menor costo; sin embargo no ofrece robustez en los aspectos de seguridad y confiabilidad de los equipos, aunado a que la información técnica con la que se describe a los equipos, no resulta suficiente para las labores del diseño de la Red.

En cualquier implementación, siempre resulta necesario saber cual es la solución que se encuentra funcionando. Resultó un tanto complicado obtener ésta información, debido a que por razones de seguridad no es viable publicar en forma detallada la estructura de la red actual, ya que algún usuario mal intencionado puede emplear de manera inapropiada lo aquí publicado. Afortunadamente se logró conseguir varios esquemas a nivel maqueta, que si bien no ofrecen los detalles que se requieren para implementar en su totalidad a la Red, resultaron útiles para el desarrollo de la propuesta. Los detalles que quedaron omitidos pueden integrarse sin ningún problema una vez aprobado el proyecto.

Durante el análisis de la infraestructura de la red LAN actual, se encontró que los equipos que están operando son compatibles con la red WLAN que se propone, pues cumplen con los requisitos mínimos necesarios para permitir la interconexión de ambas redes: los puertos disponibles cuentan con la velocidad de transmisión adecuada, permiten la autenticación de usuarios así como la gestión de VLAN's y diversos protocolos de seguridad. Sólo en uno de los casos se emite una recomendación para sustituir un equipo.

El diseño fue probado en un software que calcula el margen del enlace, que se trata de un valor medido en decibeles indicando si el enlace será funcional o no. Introduciendo los datos proporcionados por los fabricantes en dicho software y en base al diseño propuesto, se obtuvo que los enlaces tendrán un margen mayor a 7 dB para todos los casos, factor que resulta aceptable y califica de *funcional* a nuestra red WLAN. Como se expresó en el capítulo 6, los valores teóricos recabados cumplen con el objetivo. De acuerdo con el software, se tendría un mejor desempeño en la Red mediante el uso de equipos marca CISCO.

El presente trabajo aportó un basto conocimiento personal acerca de las Redes Inalámbricas, porque en los inicios de la presente investigación ésta tecnología era en su mayoría desconocida para mi persona, lo cual me conduce a pensar que para muchas otras aún lo sea, ya que las WLAN's son relativamente nuevas y la presencia en el mercado apenas se ha hecho notar desde hace un par de años en

nuestro país. En contraste, las redes LAN tradicionales tienen más de 20 años dentro del mercado mundial.

Faltaría comprobar mediante la implementación directa, que los cálculos realizados son correctos. Los ajustes que se deberán realizar cuando sea aprobada la propuesta serán necesarios porque los modelos, precios y el presupuesto asignado al proyecto pueden variar en un cierto tiempo. Además, las investigaciones para mejorar el desempeño de las WLAN's continúan día con día, dando como resultado la creación de nuevos métodos y aplicaciones que resolverían algunos problemas que persisten hoy en día. A partir de esto, se pueden abrir nuevas líneas de investigación acerca del trabajo en campo que se debe realizar una vez que se tengan los equipos listos para ser utilizados.

Desde la perspectiva académica, esta tesis permitirá ser una guía estructurada acerca de las WLAN's, desde sus inicios hasta la actualidad, y describiendo la mayor parte de sus mecanismos de operación. De manera profesional, constituye una sólida propuesta que de ser aprobada, tendrá como principal beneficio la descentralización de los centros de cómputo utilizados por la comunidad estudiantil. Así colocaríamos a la vanguardia tecnológica los servicios e instalaciones con las que cuenta actualmente la Facultad de Ingeniería y nuestra Universidad Nacional Autónoma de México.

**¡MÉXICO, PUMAS, UNIVERISDAD!**
Ciudad Universitaria
Octubre de 2005

# Bibliografía

## Capítulo Uno


Bates, Bud. Ranade, Jay. "Wireless Networked Communications". McGraw Hill. USA, 1994.

Can we use it for Multimedia?
http://information.soongsil.ac.kr/~ieee/multimedia/mu1998/u2084.pdf

El Estándar 802.11
http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

Entendiendo las Wireless LAN
http://www.kernelpanik.org/docs/kernelpanik/Wireless.pdf

Exploring Wireless Technologies
http://stsystems2002.net/nss-folder/wirelessnetworking/exploringwireless.pdf

High Performance Wireless Ethernet
http://www.csie.ncnu.edu.tw/~ccyang/WirelessNetwork/Papers/802.11/802.11Intro-3.pdf

WirelessNetworks Ready for the Enterprise
http://www.cisco.com/warp/public/784/packet/apr02/pdfs/p32-cover.pdf


## Capítulo Dos


802.11b White Paper
http://www.vocal.com/white_paper/ieee_802.11b_wp1pdf.pdf

A Condensed Review of Spread Spectrum. Techniques for ISM Band Systems
http://www.eetasia.com/ARTICLES/2001MAY/2001MAY28_NTEK_RFD_AN1.PDF

Comparison of QPSK/QAM OFDM and Spread Spectrum for the 2-11 GHz PMP BWAS
http://www.ieee802.org/16/tg3/contrib/802163c-00_23.pdf

Complementary Code Keying Made Simple
http://www.eetasia.com/ARTICLES/2001MAY/2001MAY25_NTEK_DSP_AN.PDF

Estudio de la capa física del 802.11
http://www.nodolujan.com.ar/syr/docs/wi-fi/802-11-PHY.pdf

High Performance Wireless Ethernet
http://www.nativei.com/heegard/papers/HR-WLAN.pdf

IEEE 802.11 Tutorial
http://howstudy.net/adhoc/adhoc_seminar/ieee802.11-tutorial_UCB.pdf

Processing Gain for Direct Sequence Spread Spectrum Communication Systems and PRISM
http://www.qsl.net/n9zia/pdf/AN9633.pdf

Pahlavan, Kaveh. "Wireless information networks". J. Wiley. USA, 1995. 572p

Spread Spectrum (SS)
http://www.sss-mag.com/pdf/Ss_jme_denayer_intro_print.pdf

## Capítulo Tres

2.4 GHz and 5 GHz WLAN: Competing or Complementary?
http://shay.ecn.purdue.edu/~mobility/TEAMS/SP02/Multimedia/Resources/24vs5Ghz.pdf

Cuadro Nacional de Atribución de Frecuencias
http://www.cofetel.gob.mx/wb2/COFETEL/COFE_Cuadro_nacional_de_atribucion_de_frecuencias

IEEE 802.11
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

IEEE 802.11a
http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

IEEE 802.11b
http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf

IEEE 802.11g
http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

New Draft Standard Clarifies Future of Wireless LAN
http://www.sss-mag.com/pdf/802_11g_whitepaper.pdf

The New Mainstream Wireless LAN Standard
http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf

## Capítulo Cuatro

IEEE 802.11
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

IEEE 802.11g
http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

IEEE 802.11a
http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

IEEE 802.11b
http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf

IEEE 802.11 Tutorial
http://howstudy.net/adhoc/adhoc_seminar/ieee802.11-tutorial_UCB.pdf

Investigation of the IEEE 802.11 Medium Access Control (MAC) Sublayer Functions
http://www.cs.binghamton.edu/~nael/research/widjaja.pdf

Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement
http://www.icg.isy.liu.se/courses/tsin01/material/WLANperf_Wu2002.pdf

## Capítulo Cinco

A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite
http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

Cisco SAFE: Wireless LAN Security in Depth
www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks
www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.pdf

IEEE 802.11i
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

Security for Next Generation Wireless LANs.
www.cisco.com/warp/public/102/wlan/nextgen.pdf

Wireless LAN Security and IEEE 802.11i
http://wire.cs.nthu.edu.tw/wire1x/WC02-124-post.pdf

Your 802.11 Wireless Network Has No Clothes
http://www.cs.umd.edu/~waa/wireless.pdf

## Capítulo Seis

802.11 Wireless LAN Performance
http://www.atheros.com/pt/whitepapers/atheros_range_whitepaper.pdf

A comparision of 802.11a and 802.11b Wireless LAN Standards
http://www.assuredcomptech.com/wireless1.pdf

Defining and Improving Data Throughput in Wireless LAN
http://ngia.rootforge.org/content/Downloads/WiFi/Papers/bband_80211_wp_throughput.pdf

Deploying 802.11 Wireless LAN's
http://www.3com.com/other/pdfs/products/en_US/wireless_lans_wp.pdf

Díaz González Eduardo. Pinelo Bolaños Paola. "Requerimientos para el Diseño de Red LAN Inalámbrica". Red corporativa de Datos Telmex. México, 2002.

Effects of Microwave Interference On IEEE 802.11
http://www.wlana.org/learn/microreliab.pdf

Link Planning for Wireless LAN (WLAN)
http://huizen.deds.nl/~pa0hoo/helix_wifi/linkbudgetcalc/wlan_budgetcalc.html

Maximizing Performance in 802.11 Wireless LANs
www.54g.org/pdf/WP2-Xpress-030617.pdf

Productos CISCO
http://www.cisco.com/en/US/products/hw/wireless/index.html

Productos 3Com
http://www.3com.com/prod/es_LA_AMER/prodlist.jsp?tab=cat&cat=13

The New Mainstream Wireless LAN Standard
http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf