ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN TECNOLÓGICA

IMPLEMENTACIÓN DE UNA RED INALÁMBRICA MEDIANTE UN "ACCESS POINT" PARA LAS OFICINAS 3 Y 4 DE PROFESORES DE LA ESFOT

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

PEDRO PABLO ENRÍQUEZ CAÑIZARES

DIRECTOR: ING. MÓNICA VINUEZA

QUITO, Septiembre 2006

DECLARACIÓN

Yo, Pedro Pablo Enríquez Cañizares, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

_____

Pedro Pablo Enríquez Cañizares

170677680-2

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Pedro Pablo Enríquez Cañizares, bajo mi supervisión.

_____

Ing. Mónica Vinueza

AGRADECIMIENTOS

A Dios por haberme dado la vida.

A mi esposa e hijos que con su amor infinito y su apoyo incondicional, me dieron fuerzas para culminar una meta más en mi vida.

A mis padres y hermanos que con su amor incondicional me apoyaron en cada momento y me alentaron para seguir adelante en toda mi vida estudiantil.

A mi Directora de Tesis Ing. Mónica Vinueza, quien con su ayuda, paciencia y dedicación ha sabido encaminar este proyecto de la mejor forma posible proporcionándome sus conocimientos y la guía necesaria para culminar este proyecto.

A la Escuela Politécnica Nacional por la formación intelectual y personal que he recibido.

Un sincero agradecimiento a todos los seres queridos que con su grano de arena hicieron posible la culminación de esta meta.

DEDICATORIA

Dedico este trabajo a Dios por su bondad infinita
Quien ha sabido darme la sabiduría necesaria
Para culminar este proyecto.

Dedico este trabajo a mi esposa e hijos quienes son los más importante en mi vida y gracias a su infinito amor, absoluta ayuda,
Y por el apoyo que me brindan en cada momento
Se pudo realizar la culminación de este proyecto.

Dedico este trabajo a mis padres quienes
Con su apoyo incondicional y su inmenso amor
Supieron con sabios consejos guiarme para poder lograr
Mis metas y objetivos.

Este trabajo va también dedicado a mis hermanos,
Por la confianza que depositaron en mi y por su amor y apoyo incondicional.

RESUMEN

Con el pasar del tiempo y con los nuevos y crecientes avances tecnológicos, cada vez las personas, empresas e instituciones crecen a la par con esto, lo que de alguna forma significa ampliaciones o readecuaciones en las instalaciones donde éstas funcionan. En este proyecto se comenzó con la detección de una necesidad en un lugar específico de la Escuela Politécnica Nacional, en las salas 3 y 4 de profesores de la ESFOT, decidiendo así implantar una solución a la necesidad detectada.

En el primer capítulo se hace un resumen de conocimientos y teoría que ayudó a la realización de este proyecto, tomando los temas necesarios y actualizados de libros, cursos y páginas de Internet.

En el segundo capítulo se hace un análisis del área donde se realizará el proyecto, los materiales y equipos a utilizarse, además de una serie de aspectos necesarios que se debe cumplir para la realización del proyecto.

Por último en el tercer capítulo se hace un análisis de los equipos existentes en el mercado, análisis técnico y económico, además se señala los aspectos y características de referencia para la toma de decisiones respecto a los equipos y materiales a utilizarse en este proyecto.

En el cuarto capítulo se determinan las conclusiones del trabajo y las recomendaciones pertinentes.

PRESENTACIÓN

La realización de este proyecto tiene como objetivo principal brindar una solución práctica para un sector determinado de la Escuela Politécnica Nacional, como son las salas 3 y 4 de Profesores de la ESFOT. Así como también proporcionar una pauta para futuras adecuaciones o ampliaciones de la red cableada de la Escuela Politécnica Nacional.

Por la facilidad que en la actualidad presentan las redes inalámbricas se pueden implementar este tipo de redes para dar solución a problemas puntuales a bajo costo.

Con este trabajo se pretende dar una guía de la utilización y configuración de un Access Point para la ampliación de una red.

CAPÍTULO 1.

PRINCIPALES DEFINICIONES TEÓRICAS SOBRE REDES WLAN

1.1. TOPOLOGÍAS DE REDES INALÁMBRICAS LAN. [8]

Las redes inalámbricas se construyen utilizando dos topologías básicas, "infraestructura" y "ad-hoc".

Una topología de infraestructura es una que amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica. El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice y el producto del proveedor. En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

Una topología ad-hoc es una en la cual se crea una red LAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de que sea a través de un controlador central. Esto es útil en lugares en donde pequeños grupos de computadoras pueden congregarse y no se necesita acceso a otra red. Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar ideas, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

1.1.1. Descripción de Funcionamiento en Modalidad de Infraestructura. [8]

Una portátil o dispositivo inteligente, que se caracteriza como una "estación" en términos inalámbricos de una red, primero tiene que identificar los puntos y las redes disponibles de acceso. Esto se hace a través del monitoreo de tramas 'beacon' desde

puntos de acceso, anunciándose así mismo o probando activamente una red en particular utilizando tramas de prueba.

La estación elige una red de las que están disponibles y sigue a través de un proceso de autenticación con el punto de acceso. Una vez que se han verificado entre sí el punto de acceso y la estación, se inicia el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y capacidades. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso en la red para dispersar conocimiento de la ubicación actual de la estación en la red. Sólo después de terminar la asociación la estación puede transmitir o recibir tramas en la red.

En la modalidad de infraestructura, todo el tráfico en red de las estaciones inalámbricas en la red pasa a través de un punto de acceso para llegar a su destino y una red LAN ya sea cableada o inalámbrica.

El acceso a la red se maneja utilizando un protocolo de telecomunicación con sensor y evasión de colisiones. Las estaciones escucharán transmisiones de datos por un período específico de tiempo antes de intentar ejecutar la transmisión - este es el componente sensor del protocolo de telecomunicación. La estación debe esperar un período específico de tiempo después de que la red quede limpia o quede lista antes de hacer la transmisión. Luego se genera un reconocimiento de la transmisión por parte de la estación receptora, indicando una recepción exitosa de la parte que evita colisión del protocolo. En esta modalidad de infraestructura, el transmisor o el receptor es siempre el punto de acceso.

Debido a que algunas estaciones no pueden escucharse entre sí, ahora que ambas están en el rango de punto de acceso, se deben hacer consideraciones especiales para evitar colisiones. Esto incluye un tipo de intercambio de reservación que puede tomar lugar antes de que se transmita un paquete, utilizando una solicitud para enviar y limpiar el intercambio de tramas, así como un vector de asignación de red que se mantenga en cada estación de la red. Aún si una estación no puede escuchar la transmisión de la otra, escuchará la autorización para enviar la transmisión desde el punto de acceso y puede evitar transmisiones durante ese intervalo.

El proceso de roaming desde un punto de acceso al otro no queda definido completamente por el estándar 802.11. Sin embargo, las guías y los sondeos que se utilizan para localizar puntos de acceso y un proceso de reasociación que permite que la estación se asocie con un punto de acceso diferente, en combinación con otros protocolos específicos de otros proveedores entre puntos de acceso, proporcionan una transición sin problemas.

La sincronización entre las estaciones en la red se maneja por las tramas periódicas enviados por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso al momento de la transmisión, de tal manera que pueden utilizarse para verificar cualquier desviación en la estación de recepción. Se requiere de sincronización por distintas razones que tienen que ver con los protocolos inalámbricos y los esquemas de modulación.

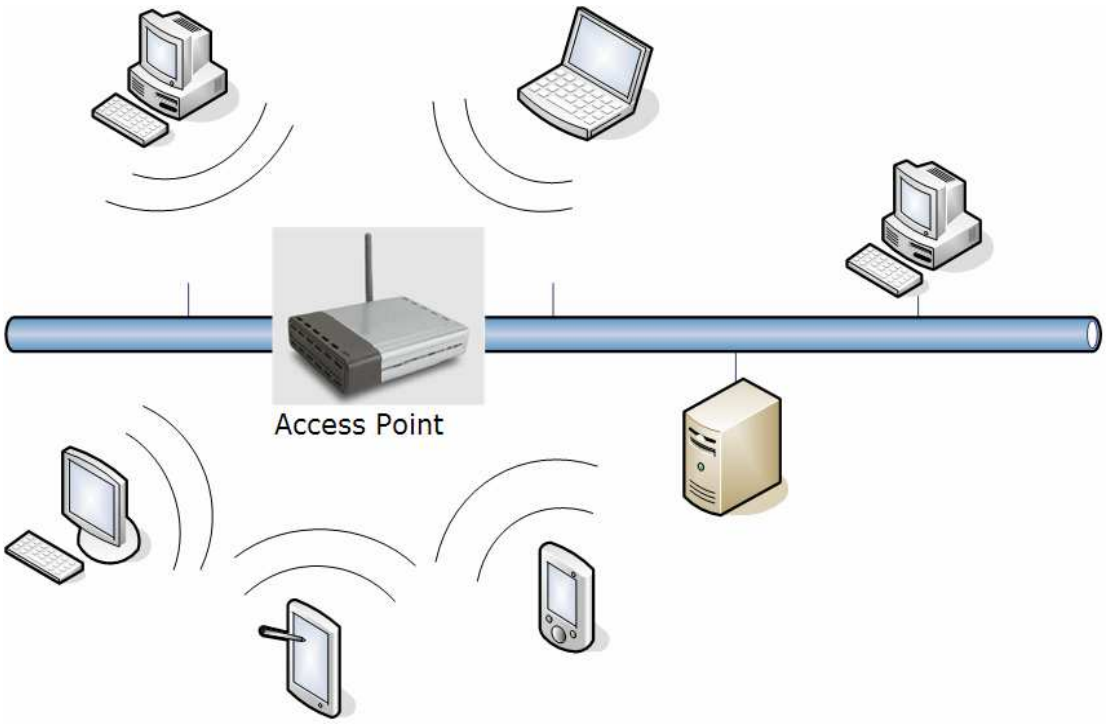


Figura 1.1. Configuración de redes LAN Inalámbrica con Infraestructura. [5]

1.1.2. Descripción de Funcionamiento en Modalidad Ad-Hoc. [8]

En la modalidad Ad-hoc simplemente no hay un punto de acceso. En esta red sólo están presentes los dispositivos inalámbricos. Muchas de las responsabilidades previamente

manejadas por el punto de acceso, como las tramas y la sincronización, las maneja una estación. Algunas mejoras no están disponibles en la red ad-hoc, como roaming entre dos estaciones que no se puedan escuchar entre sí.

Una red Ad-Hoc es una red entre iguales (sin servidor central o punto de acceso) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computador, puede reunirse para una cita de negocios o para una conferencia, conectando sus computadoras en una red temporal durante la reunión.

Observando la *figura 1.1* y la *figura 1.2* se entiende las diferencias entre una LAN Inalámbrica Ad-Hoc y una red inalámbrica que proporciona ampliaciones de LAN y acceso nómada.

El modo ad-hoc se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red ad-hoc consta de un máximo de 9 clientes inalámbricos, que se envían los datos directamente entre sí. En la *figura 1.2.* se muestra una red inalámbrica en modo ad hoc. [7]

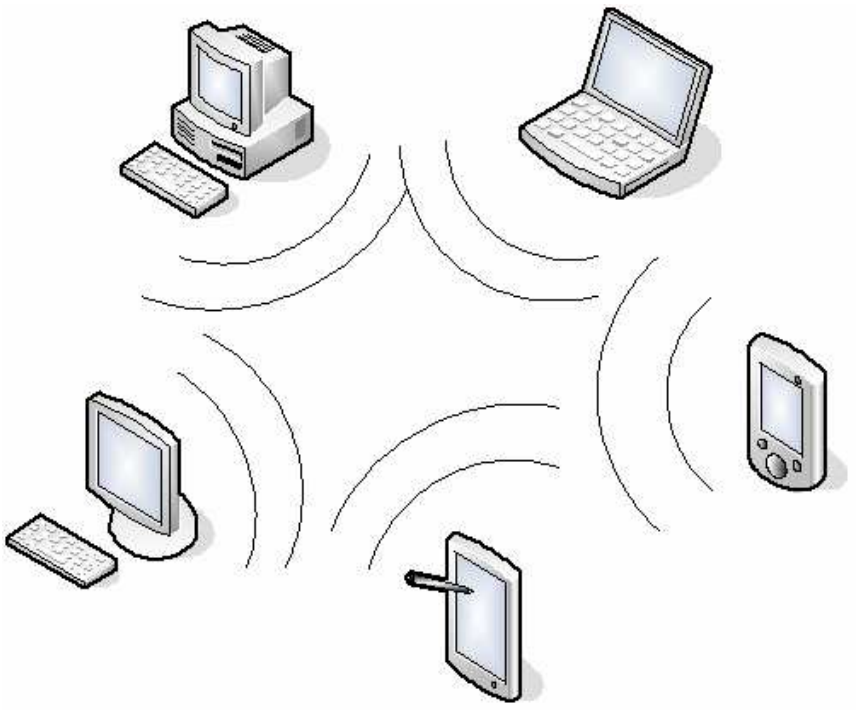


Figura 1.2. Configuración de redes LAN Inalámbrica "ad-hoc". [5]

1.2. VENTAJAS Y DESVENTAJAS.

1.2.1. Ventajas de las Redes LAN Inalámbricas. [6]

Movilidad.

Los usuarios tienen la libertad para movilizarse, mientras todavía permanecen conectados. Las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas. La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada.

Costo de propiedad reducido.

Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN cableada, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad.

Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

Flexibilidad.

Existen ambientes que por circunstancias de cambio, mejoras o crecimiento están sujetos a cambios de la configuración física y a expansiones frecuentes de sus instalaciones, las WLAN permiten hacer muy fácilmente este tipo de cambios y expansiones. Esta flexibilidad se debe a que el medio de transmisión que se utiliza es “el aire”, el único cambio físico se lo hace en la reubicación o aumento de usuarios dependiendo del caso, además las WLAN no incurrirán en costos de re-cableado durante las modificaciones de la configuración de las oficinas.

Facilidad de Instalación.

Las WLAN pueden usarse para proporcionar la conectividad de sitio a sitio hasta 25 millas. Además pueden proporcionar la conectividad entre sitios que están separados por barreras físicas o geográficas que harían imposible la instalación de un medio de comunicación físico. Para las WLAN es muy fácil realizar su implementación, no necesita de medios de transmisión físicos, por esta razón no es necesario realizar ninguna obra civil que implicaría una red cableada.

1.2.2. Desventajas de las Redes LAN Inalámbricas. [13]

- Una de las principales desventajas que tienen las redes LAN inalámbricas en general es que algunos sistemas pueden llegar a afectar a la salud de los usuarios, no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico.
- Se puede decir también que una desventaja es la velocidad de transmisión de datos a la que trabajan las redes LAN inalámbricas frente a la velocidad que alcanzan los datos en las redes cableadas.
- Lenta evolución. A pesar de su importancia, desde un punto de vista tecnológico y estratégico (el paso de la telefonía móvil a la computación móvil, las perspectivas de un multimedia móvil o la banda ancha en el contexto móvil), el mercado de las redes LAN inalámbricas ha evolucionado muy lentamente, sin obedecer a las expectativas generadas en los últimos años, que hablaban de importantes crecimientos de negocio. Esto se ha debido, entre otros motivos, a los propios problemas que siempre conlleva el nacimiento de una tecnología: los desequilibrios entre la oferta y la demanda y la debilidad del modelo de relaciones, asociado, los problemas de excelencia de la propia tecnología (las prestaciones de los productos o servicios),

1.3. APLICACIONES DE LAS REDES LAN INALÁMBRICAS. [6]

Las aplicaciones de las redes inalámbricas están divididas en dos grupos importantes, esta clasificación hace referencia al tipo de mercado en el que se las aplica. Lo dos grupos principales son:

- **Aplicaciones Verticales:** Se refieren a las soluciones a problemas específicos en fábricas, clínicas y hospitales, en usuarios hogar y en proyectos educativos.
- **Aplicaciones Horizontales:** Se refieren a soluciones corporativas en ampliaciones de redes cableadas, implementación de nuevas redes acopladas a la red principal de una empresa, provisión de servicios de conexión a trabajadores de campo.

1.3.1. Aplicaciones Verticales. [6]

- ✓ Retail
- ✓ Almacenes
- ✓ Tecnología y Electrónica
- ✓ Gobierno
- ✓ Cuidado de la salud
- ✓ Seguros
- ✓ Bienes raíces
- ✓ Transporte
- ✓ Delivery (el tren, tierra, la nave, el aire)
- ✓ La Hospitalidad & las Convenciones
- ✓ Servicios (Agua, Gas, Electricidad)
- ✓ Banca & finanzas
- ✓ Ventas
- ✓ Empresarial e Industrial
- ✓ Educación
- ✓ Viajes & Recreación
- ✓ Aplicaciones Militares

Cuatro factores principales manejan la aceptación creciente de tecnología inalámbrica:

- **Velocidad:** 11 Mbps, 54 Mbps y actualmente hasta 108 Mbps se estandarizan para un mejor rendimiento en reuniones importantes.

- **Posicionamiento**: Posicionando las Redes del Área Local Inalámbricas como un medio para completar las LAN/WAN cableadas, conectando a esta red de computadoras una solución a varios problemas de movilidad de usuarios y expansión de la red. También anima que clientes incluyan la tecnología inalámbrica en su gestión estratégica de redes.
- **Costos**: Bajos costos de instalación con alto rendimiento hacen a una red inalámbrica una alternativa más atractiva que las soluciones cableadas.
- **Facilidad de Instalación:** Soluciones instantáneas y alternativas fácilmente llevadas a cabo aceleran la adopción del mercado de redes inalámbricas.

El mercado de las redes inalámbricas está constantemente creciente y en desarrollo. La innovación tecnológica y la reciente regularización están poniendo el fundamento para la adopción del mercado.

Las características inalámbricas, mejor rendimiento, más bajos costos y facilidad de implementación están acelerando el crecimiento del mercado.

1.3.2. Aplicaciones Horizontales. [6]

- Extender las redes cableadas para proporcionar la movilidad de los usuarios.
- Eliminar los problemas de la instalación y altos costos de una red cableada.
- Proveer una solución de la gestión de redes completa para las pequeñas empresas y hogares.
- Integrar hogar, viajes y ambientes de trabajo para lograr conectividad flexibilidad, consistencia a los usuarios.
- Superar restricciones físicas que limitan la expansión de una red.
- Proveer variedad y prontas soluciones LAN en ambientes de constante cambio.
- Profesionales o ejecutivos de negocio que quieren la movilidad dentro de la empresa, quizás, además de una red cableada tradicional.
- Dueños de Comerciales o Gerentes que necesitan la flexibilidad por los frecuentes cambios en su red LAN cableada a lo largo de su empresa o en áreas seleccionadas.

- Empresas cuyo sitio no es adecuado a una LAN cableada debido a que se debe construir: con presupuestos limitados, en edificios muy viejos, en locales arrendados o en sitios temporales.
- Empresas que necesita la flexibilidad y los ahorros de costos que ofrece la implementación de conexión mediante línea de vista entre edificios, para evitar excavaciones caras, arrendamiento de medios de transmisión, o pagos por derecho de vías con el gobierno.

1.4. AMPLIACIÓN DE LAS REDES LAN MEDIANTE REDES INALÁMBRICAS. [4]

Los primeros productos de LAN inalámbricas, aparecidos a finales de los años ochenta, eran ofrecidos como sustitutos de las redes LAN cableadas tradicionales. Una red LAN inalámbrica evita el costo de la instalación del cableado y facilita las tareas de traslado y modificaciones en la estructura de la red. Sin embargo, esta motivación de las LAN inalámbricas fue superada por los acontecimientos. En primer lugar, a medida que la necesidad de las redes LAN se hizo cada vez más patente, los arquitectos incluyeron en el diseño de los nuevos edificios un extenso cableado para aplicaciones de datos.

Además, con los avances en la tecnología de transmisión de datos se ha incrementado la dependencia con los pares trenzados para redes LAN, especialmente con los UTP de categoría 3 y categoría 5. Así, dado que la mayor parte de los edificios viejos estaban ya cableados con par trenzado de categoría 3, y muchos de los edificios de nueva construcción lo están con par trenzado categoría 5, resulta escaso el uso de LAN inalámbricas como sustituto de las LAN cableadas.

Sin embargo, el papel de una LAN inalámbrica como alternativa a las LAN cableadas es importante en un gran número de entornos.

Algunos ejemplos son edificios que poseen una gran superficie, como plantas de fabricación, plantas comerciales y almacenes, edificios históricos con insuficiente cable de par trenzado y en los que está prohibido hacer más agujeros para introducir nuevo cableado, y en pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan rentables. En todos estos casos, una LAN inalámbrica ofrece una alternativa efectiva y más atractiva. En la mayor parte de estas situaciones, una organización dispondrá también de una LAN cableada con servidores y algunas

estaciones de trabajo estacionarias. Por ejemplo, una planta de manufacturación dispone, generalmente, de una oficina independiente de la propia planta, pero que debe estar interconectada con ella con el fin de proporcionar trabajo en red.

Por tanto, una LAN inalámbrica está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de redes LAN.

En la *figura 1.3.* se muestra una configuración sencilla de una LAN inalámbrica típica en muchos entornos.

Existe una LAN troncal cableada, como una ethernet, que conecta varios servidores, estaciones de trabajo y uno a más puentes o dispositivos de encaminamiento para la comunicaron con otras redes.

Adicionalmente, existe un módulo de control (CM, Control Module) que funciona como interfaz con la LAN inalámbrica. El módulo de control incluye funciones propias de un puente o de un dispositivo de encaminamiento para conectar la LAN inalámbrica con la troncal.

Además, se incluye un tipo de lógica de control de acceso, como por ejemplo un esquema de sondeo o uno de paso de testigo, para regular el acceso de los sistemas finales.

Hemos de destacar que algunos de los sistemas finales son dispositivos independientes, como estaciones de trabajo y servidores. Los concentradores (hub) u otros módulos de usuario (UM, User Module) que controlan varias estaciones fuera de una LAN cableada pueden también formar parte de la LAN inalámbrica.

Las configuraciones de la *figura 1.3.* se denominan LAN inalámbrica de celda única, ya que todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control. Otra configuración común, sugerida en la *figura 1.4.*, es una LAN inalámbrica de celdas múltiples.

En este caso existen varios módulos de control interconectados por una LAN cableada.

Cada módulo de control da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión. Por ejemplo, con una LAN de infrarrojos, la transmisión se encuentra limitada a una sola habitación, por lo que se necesita una celda en cada habitación de un edificio de oficinas que precise de soporte inalámbrico.

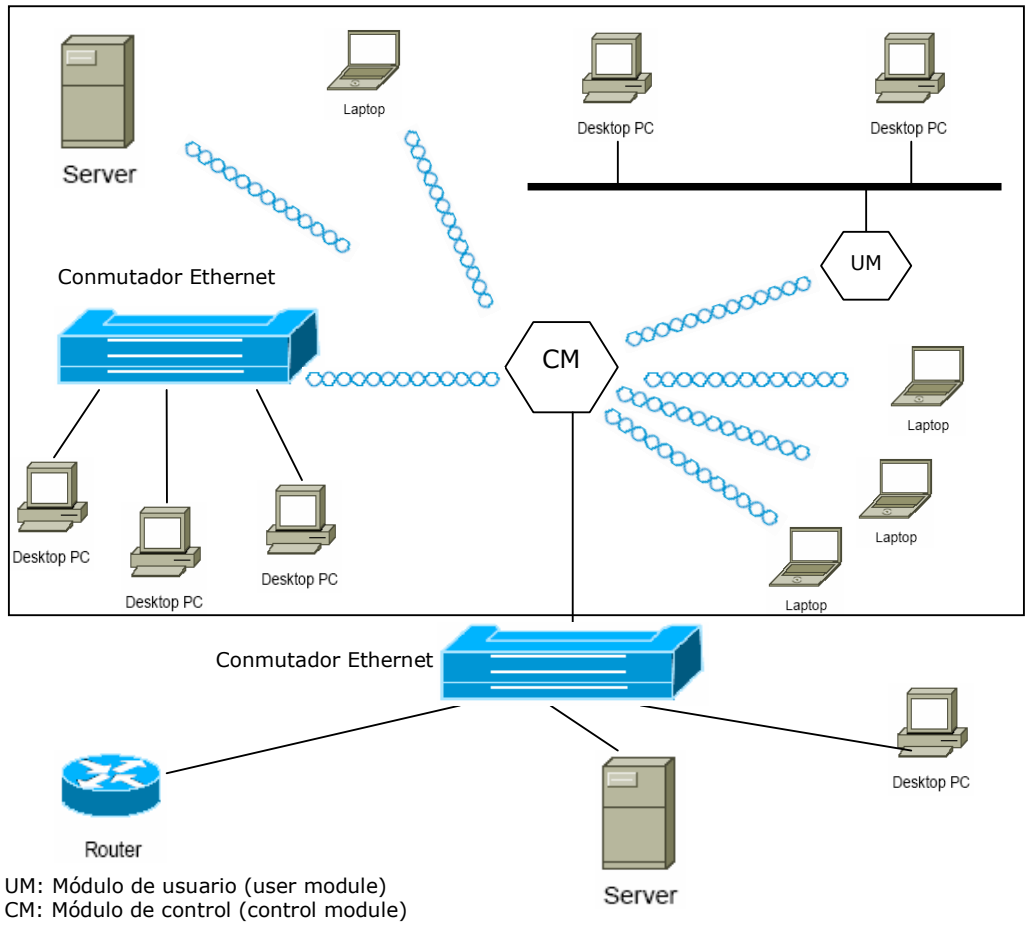


Figura 1.3. Ejemplo de una LAN inalámbrica de celda única. [4]

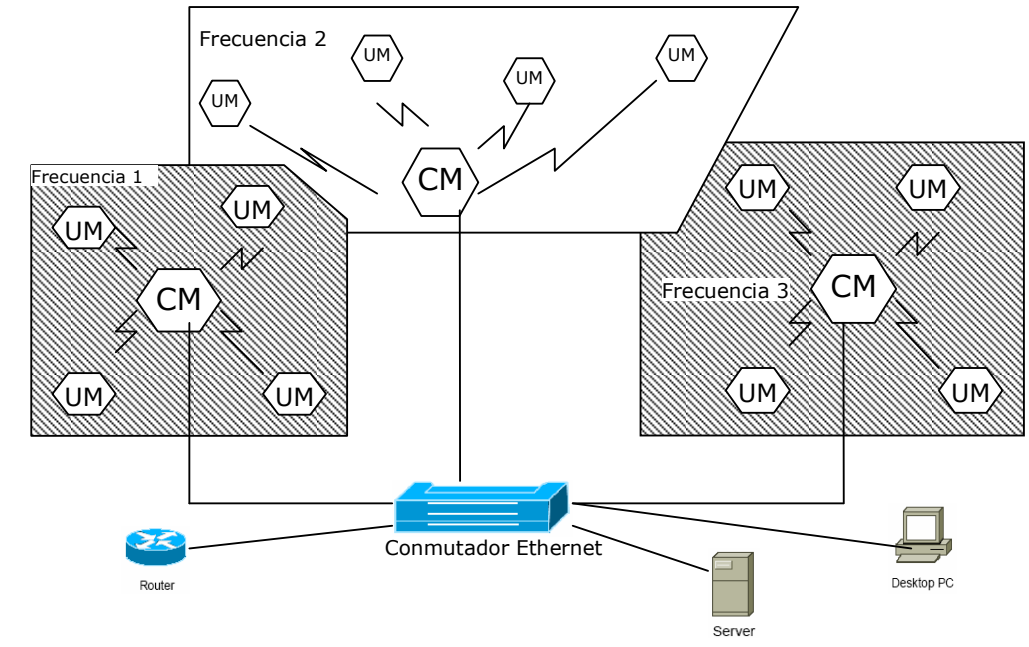


Figura 1.4. Ejemplo de una LAN Inalámbrica de celdas múltiples. [4]

1.5. REQUISITOS DE LAS REDES LAN INALÁMBRICAS. [6]

Los cuatro requisitos principales para una solución de una red inalámbrica son: disponibilidad, escalabilidad, manejabilidad, y debe ser una arquitectura abierta.

Disponibilidad

Alta disponibilidad se logra a través de la redundancia del sistema y del diseño de área de cobertura apropiado. La redundancia de Sistema incluye Access Points redundantes en frecuencias separadas. El diseño apropiado del área de cobertura incluye cuentas para "roaming", negociación automática cuando la fuerza de señal se debilita, la selección de la antena apropiada y posiblemente el uso de un repetidor para extender el área de cobertura dónde un Access Point no puede usarse. Soporte para movilidad no sólo dentro de una subred sino también para las subredes entre edificios o entre "campus" también es necesario.

Escalabilidad.

La escalabilidad es lograda apoyada por varios "Access Points" en un área de cobertura que usa frecuencias múltiples o modelo del brinco. Los "Access Points" también pueden realizar el equilibrio de frecuencias deseado.

Manejabilidad.

Las herramientas diagnóstico representan una gran administración dentro de redes inalámbricas. Los clientes necesitan para administrar la red inalámbrica dispositivos "Access Points" normales (SNMP Simplified Network Management Protocol, Web) o a través de la administración de empresas mediante las aplicaciones como Cisco Works 2000, Cisco Stack Manager o Cisco Resource Monitor, etc.

Cuando las tecnologías inalámbricas están incorporadas en las grandes empresas con redes, lo concerniente a la administración debe ser dirigido. Lo concerniente a la facilidad de la implementación, la facilidad de mantenimiento, y cuando los problemas suceden tan fácil es arreglar y resolver los problemas.

Arquitectura Abierta.

Una arquitectura abierta permite la integración equipos de terceros o de diferentes fabricantes. Esta forma de acoplarse se logra mediante la normalización y los

estándares (como 802.11b), participación en las asociaciones de interoperabilidad (como WECA), y la certificación (como la certificación de FCC Federal Communications Commission).

Otros requisitos están evolucionando para que las tecnologías de red inalámbricas ganen la popularidad:

Seguridad.

Es esencial encriptar paquetes de datos transmitidos a través de un medio de libre acceso como es el aire. En instalaciones más grandes, autenticación de los usuarios centralizada y administración centralizada en que se requieran claves encriptadas.

Rendimiento.

Se espera que el rendimiento continúe aumentando en velocidad de datos de 54 a 108 Mbps en la banda de 2.4 GHz, con una visión a las velocidades superiores (54 Mbps y superiores) en la banda de 5 GHz.

Costos.

Los clientes esperan las reducciones continuas en los costos (15-30% cada año) a lo largo del incremento del rendimiento. Los clientes no están interesados sólo con el precio de compra sino también con el costo total del capital, incluso el costo de la instalación en los techos y otros lugares de difícil acceso.

Estándares.

Con el estándar IEEE 802.11b, la interoperabilidad entre tercera generación de fabricantes está volviéndose una realidad. Cuando las tecnologías inalámbricas evolucionan en las nuevas áreas con velocidades de datos superiores, la regularización e interoperabilidad estarán preocupando continuamente a las organizaciones encargadas de los estándares.

1.6. PROTOCOLOS DE LAS REDES LAN INALÁMBRICAS.

1.6.1. Modelo OSI y Protocolos. [5]

Todos los estándares inalámbricos se basan el modelo de OSI (Open System Interconnection) realizado por la ISO (International Standards Organization).

Los estándares están dentro de las dos capas más bajas del modelo OSI y son compatibles con 802.2.

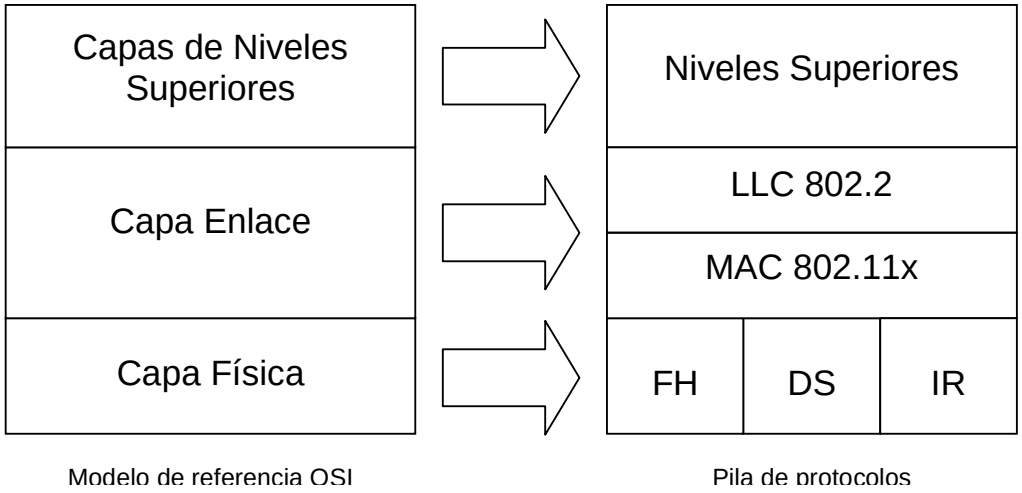


Figura 1.5. Modelo OSI y Protocolos 802.11. [5]

LLC: Control Lógico del Enlace (Logical Link Control)

MAC: Control de Acceso al Medio (Medium Access Control)

FHSS: Espectro Ensanchado por Saltos de Frecuencia (Frequency Hopping Spread Spectrum)

DSSS: Espectro Ensanchado por Secuencia Directa (Direct Sequence Spread Spectrum)

IR: Infrarrojo (InfraRed)

Protocolos de las LAN Inalámbricas. [1]

A medida que crece la cantidad de dispositivos de cómputo y comunicación portátiles, también crece la demanda de conexión de ellos con el mundo externo. Los primeros teléfonos portátiles ya tenían la capacidad de conectarse con otros teléfonos. Las primeras computadoras portátiles no tenían esta capacidad, pero poco después los módems se volvieron comunes en tales computadoras. Para entrar en línea, estas computadoras tenían que conectarse a un enchufe telefónico. El requisito de una conexión con cable a la red fija significó que las computadoras eran portátiles, más no móviles.

Para lograr una auténtica movilidad, las computadoras portátiles necesitan usar señales de radio (o infrarrojos) para comunicarse. De esta manera, los usuarios pueden leer y enviar correo mientras van de excursión o navegan. Un sistema de computadoras portátiles que se comunican por radio pueden considerarse una LAN inalámbrica. Estas

LAN tienen propiedades un tanto diferentes que las LAN convencionales o cableadas y requieren protocolos de subcapa MAC especiales.

Una configuración común para las LAN inalámbricas es un edificio de oficinas con estaciones base (también conocidos como puntos de acceso “Access Points”) ubicados estratégicamente en distintas partes del edificio. Todas las estaciones base están interconectadas mediante cobre o fibra. Si la potencia de transmisión de las estaciones base y portátiles se ajusta a un alcance de 3 o 4 metros, entonces cada cuarto se vuelve un a celda única, y el edificio se vuelve un sistema celular grande, como los sistemas de telefonía celular tradicionales. A diferencia de los sistemas telefónicos celulares, cada celda solo tiene un canal, que cubre todo el ancho de banda disponible. Por lo general el ancho de banda es de 11 a 54 Mbps.

Para usar una LAN inalámbrica se puede utilizar el CSMA Carrier Sense Multiple Access; escuchar si hay otras transmisiones y solo transmitir solo si nadie más lo esta haciendo. El problema radica en que este protocolo no es realmente adecuado porque lo que importa es la interferencia en el receptor, no en el emisor. Para ver la naturaleza de este problema, considere la siguiente ilustración, en la que se muestran 4 estaciones inalámbricas. Para nuestros fines, no importa cuales son estaciones base ni cuales son portátiles. Es alcance de radio es tal que *A* y *B* están en el mismo alcance y potencialmente pueden interferir entre sí. *C* también podría interferir tanto con *B* como con *D*, pero no con *A*.

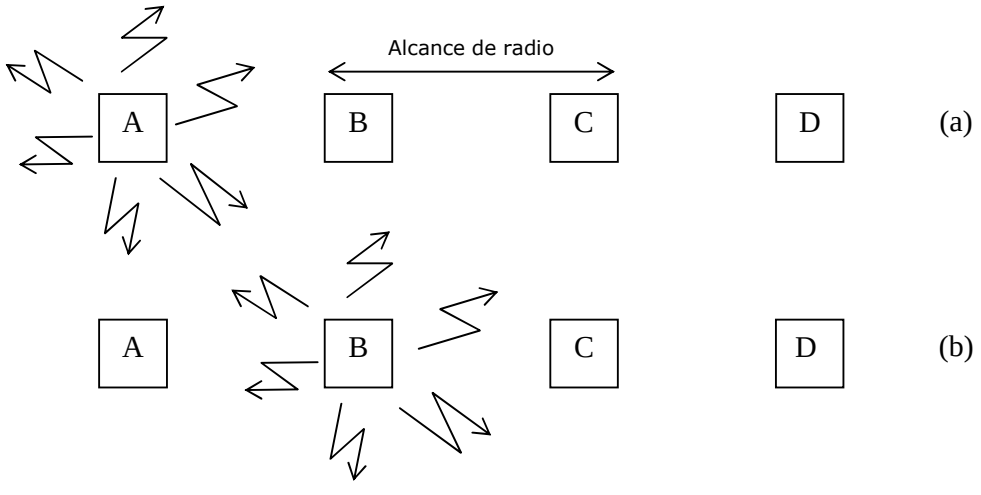


Fig. 1.6. LAN inalámbrica. (a) A transmitiendo. (b) B transmitiendo. [1]

Primero se considera lo que ocurre cuando *A* está transmitiendo hacia *B*, como se muestra en la *figura 1.6. (a).* Si *C* detecta el medio, no podrá escuchar a *A* porque está fuera de su alcance y, por tanto, deducirá falsamente que puede transmitir a *B.* Si *C* comienza a transmitir, interferirá *B*, eliminando la trama de *A.* El problema de que una estación no puede detectar a un competidor potencial por el medio, puesto que dicho competidor está demasiado lejos, se denomina **problema de estación oculta.**

Ahora se considera la situación inversa: *B* transmitiendo a *A*, como se muestra en la *figura 1.6. (b).* Si *C* detecta el medio, escuchará una transmisión y concluirá equivocadamente que no puede enviar a *D*, cuando de hecho tal transmisión causaría una mala recepción solo en la zona entre *B* y *C*, en la que no está localizado ninguno de los receptores pretendidos. Esta situación se denomina **problema de estación expuesta**.

El problema es que antes de comenzar una transmisión, una estación realmente necesita saber si hay actividad o no alrededor del receptor. El CSMA simplemente le indica si hay o no actividad alrededor de la estación que está detectando la portadora. Con un cable, todas las señales se propagan a todas las estaciones, de manera que sólo puede llevarse a cabo una transmisión en un momento dado en cualquier lugar del sistema. En un sistema basado en ondas de radio corto alcance, pueden ocurrir transmisiones simultáneas si las ondas tienen destinos diferentes y éstos están fuera de alcance entre sí.

Otra forma de visualizar este problema es imaginar un edificio de oficinas en el que cada empleado tiene una computadora portátil inalámbrica. Suponga que *Usuario 1* quiere enviar un mensaje a *Usuario 2*. La computadora de *Usuario 1* detecta el entorno local y, al no percibir actividad, procede a transmitir. Sin embargo, aún puede hacer colisión en la oficina de *Usuario 2*, pues un tercero podría estar transmitiéndole actualmente desde una localidad tan alejada de la de *Usuario 1* que la computadora de éste no podrá detectarlo.

1.6.2. MACA Y MACAW. [1]

MACA (Acceso Múltiple con Prevención de Colisiones) (Karm, 1990) es uno de los primeros protocolos diseñados para las LAN inalámbricas. El concepto en que se basa es que el emisor estimule al receptor a enviar una trama corta, de manera que las

estaciones cercanas puedan detectar esta transmisión y eviten ellas mismas hacerlo durante la siguiente trama de datos (grande). El MACA se ilustra en la *figura 1.7.*

Se considera ahora la manera en que *A* envía una trama a *B. A* comienza por enviar una trama RTS (Request To Send) (solicitud de envío) a *B*, como se muestra en la *figura 1.7. (a).* Esta trama corta (30 bytes) contiene la longitud de la trama de datos que seguirá posteriormente. Después *B* contesta con una trama CTS (Clear To Send) (libre para envío), como se muestra en la *figura 1.7. (b).* La trama CTS contiene la longitud de los datos (copiada de la trama RTS). Una vez que sucede la recepción de la trama CTS, *A* comienza a transmitir.

Ahora se verá cómo reaccionan las estaciones que escuchan cualquiera de estas tramas. Cualquier estación que escuche el RTS evidentemente está bastante cerca de *A* y debe permanecer en silencio durante el tiempo suficiente para que el CTS se transmita de regreso a *A* sin conflicto. Cualquier estación que escuche el CTS está bastante cerca de *B* y debe permanecer en silencio durante la siguiente transmisión de datos, cuya longitud puede determinar examinando la trama CTS.

En la *figura 1.7. C* está en el alcance de *A*, pero no en el de *B.* Por tanto, escucha el RTS de *A* pero no el CTS de *B.* Mientras no interfiera con el CTS, está libre para transmitir mientras se está enviando la trama de datos. En contraste, *D* está en el alcance de *B* pero no de *A.* No escucha el RTS de A pero si el CTS de B. Al escuchar el CTS se le indica que está cerca de una estación que está a punto de recibir una trama, por lo que difiere el envío de cualquier cosa el momento que se espera la terminación de esa trama. La estación *E* escucha ambos mensajes de control y, al igual que *D*, debe permanecer en silencio hasta que se haya completado la trama de datos.

A pesar de estas precauciones, aun pueden ocurrir colisiones. Por ejemplo, *B* y *C* pueden enviar tramas RTS a *A* al mismo tiempo. Estas chocarán y se perderán. En el caso de una colisión, un emisor sin éxito (es decir, uno que no escucha un CTS en el intervalo de tiempo esperado) espera un tiempo aleatorio y reintenta. El algoritmo empleado es el retroceso exponencial binario, que estudiaremos cuando lleguemos a ethernet.

Con base en estudios de simulación de MACA, Bharghavan y Cols (1994) afinaron el MACA para mejorar su desempeño y llamaron **MACAW (MACA Inalámbrico)** a su nuevo protocolo. Para comenzar, notaron que, sin confirmación de recepción de la capa

de enlace de datos, las tramas no eran retransmitidas sino hasta que la capa de transporte notaba su ausencia, mucho después. Resolvieron el problema introduciendo una trama ACK tras cada trama de datos exitosa. También observaron que CSMA puede servir para evitar que una estación transmita un RTS al mismo tiempo y destino que otra estación cercana, por lo que se agrego la detección de portadora. Además, decidieron ejecutar el algoritmo de retroceso por separado para cada flujo de datos (par origen-destino), en lugar de para cada estación. Este cambio mejora la equidad de protocolo. Por último, agregaron un mecanismo para que las estaciones intercambiaran información sobre congestionamientos, y una manera de hacer que el algoritmo de retroceso reaccionara menos violentamente a problemas pasajeros, con lo que mejoraron el desempeño del sistema.

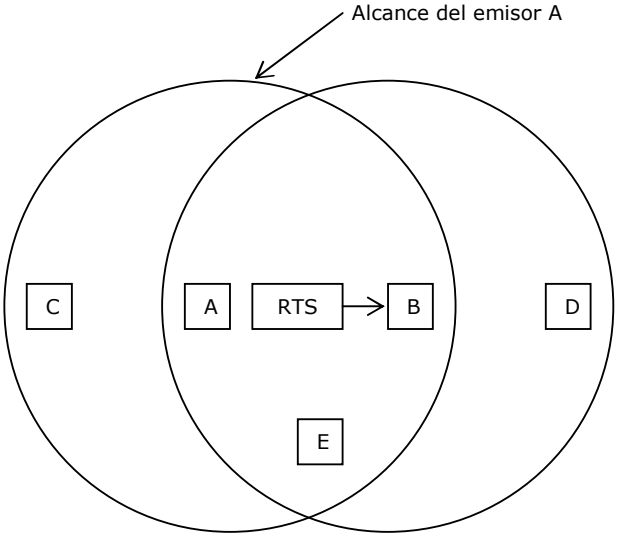


Figura 1.7. (a). El protocolo MACA. A enviando a B un RTS. [1]

1.6.3. El protocolo de la subcapa MAC de 802.11. [1]

El protocolo de la subcapa MAC para el estándar 802.11 es muy diferente del de Ethernet debido a la complejidad inherente del entorno inalámbrico en comparación con el de un sistema cableado. Con ethernet, una estación simplemente espera hasta que el medio queda en silencio y comienza a transmitir. Si no recibe una ráfaga de ruido dentro de los primeros 64 bytes, con seguridad la trama ha sido entregada correctamente. Esta situación no es válida para los sistemas inalámbricos.

Para empezar, existe el problema de la estación oculta mencionado con anterioridad, el cual se ilustra nuevamente en la *figura 1.9. (a).*

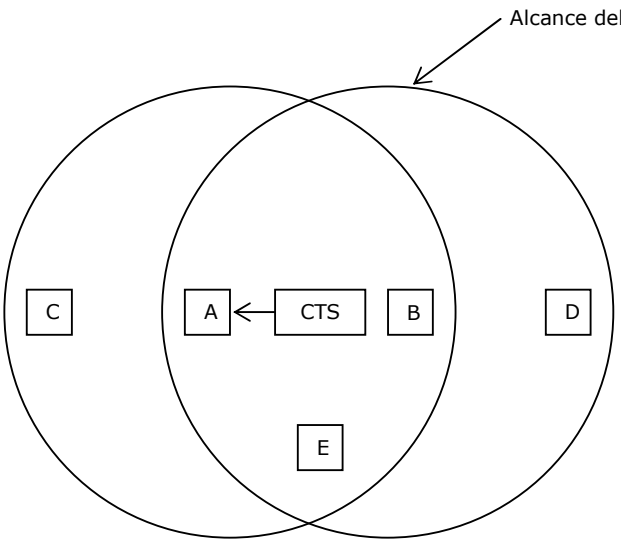


Figura 1.8. (b). El protocolo MACA. B respondiendo a A con un CTS. [1]

Puesto que no todas las estaciones están dentro del alcance de radio de cada una, las transmisiones que van en un lado de una celda podrían no recibirse en otro lado de la misma celda. En este ejemplo, la estación *C* transmite a la estación *B*. Si *A* detecta el canal, no escuchará nada y concluirá erróneamente que ahora puede comenzar a transmitir a *B*.

Además, existe el problema inverso, el de la estación expuesta, que se ilustra en la *figura 1.8. (b)*. Aquí *B* desea enviar a *C* por lo que se escucha el canal. Cuando escucha una transmisión, concluye que no debería transmitir a *C*, aunque *A* esté transmitiendo a *D* (lo cual no se muestra). Además, la mayoría de los radios son semiduplex, lo que significa que no pueden transmitir y escuchar ráfagas de ruido al mismo tiempo en una sola frecuencia. Como resultado de estos problemas, 802.11 no utiliza CSMA/CD, como lo hace Ethernet.

Para solucionar este problema, 802.11 soporta dos modos de funcionamiento. El primero, llamado **DCF (Función de Coordinación Distribuida)**, no utiliza ningún tipo de control central (en ese aspecto, es similar a Ethernet). El otro, llamado **PCF (Función de Coordinación Puntual)**, utiliza la estación base para controlar toda la actividad en su celda. Todas las implementaciones soportan DCF pero PCF es opcional. A continuación se analiza estos dos modos a la vez. Cuando se emplea DCF, 802.11 utiliza un protocolo llamado **CSMA/CA (CSMA con Prevención de Colisiones)**.

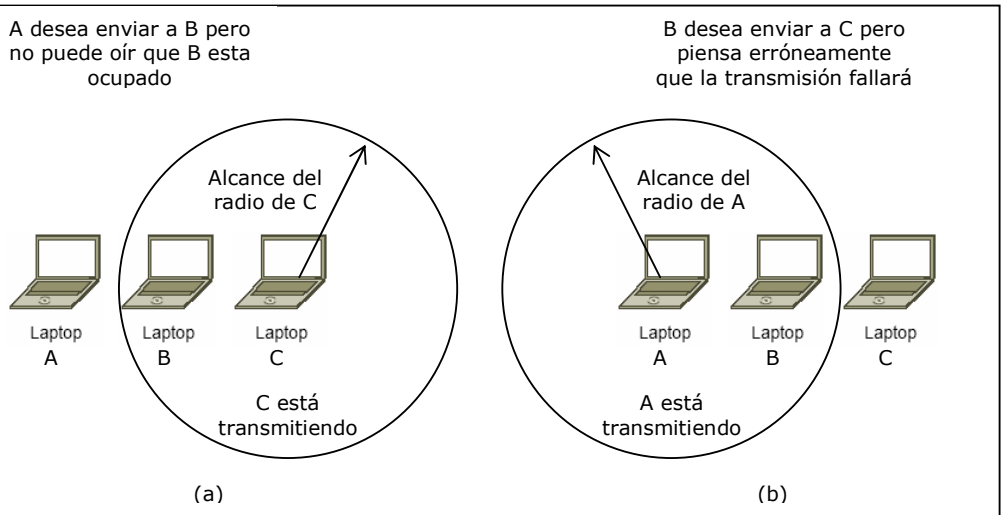


Figura 1.9. (a) El problema de la estación oculta. (b) El problema de la estación expuesta. [1]

Es este protocolo, se utiliza tanto la detección del canal físico como la del canal virtual. Los dos métodos de funcionamiento son soportados por CSMA/CA. En el primer método, cuando una estación desea transmitir, detecta el canal. Si está inactivo, comienza a transmitir. No detecta el canal mientras transmite pero emite su trama completa, la cual podría ser destruida en el receptor debido a interferencia. Si el canal está ocupado, el emisor espera hasta que esté inactivo para comenzar a transmitir. Si ocurre una colisión, las estaciones involucradas en ella esperan un tiempo aleatorio, mediante el algoritmo de retroceso exponencial binario de Ethernet, y vuelve a intentarlo más tarde.

El otro modo de la operación CSMA/CA se basa en MACAW y utiliza la detección de canal virtual, como se ilustra en la *figura 1.10.* En este ejemplo, *A* desea enviar a *B*. *C* es una estación que está dentro del alcance de *A* (y posiblemente del alcance de *B*, pero eso no importa). *D* es una estación dentro del alcance de *B* pero no dentro del de *A*.

El protocolo inicia cuando *A* decide enviar datos a *B*. A inicia enviándole una trama RTS a *B* en la que solicita permiso para enviarle una trama. Cuando *B* recibe esta solicitud, podría decidir otorgarle el permiso, en cuyo caso le regresa una trama CTS. Al recibir la CTS, *A* ahora envía su trama y comienza a temporizar de ACK. Al recibir correctamente la trama de datos, *B* responde con una trama de ACK, con lo que termina el intercambio. Si el temporizador de ACK de *A* termina antes de que el ACK regrese, todo el protocolo se ejecuta de nuevo. Ahora se considera este intercambio desde el punto de vista de *C* y *D*. *C* está dentro del alcance de *A*, por lo que podría recibir la trama RTS. Si pasa esto, se da cuenta de que alguien va a enviar datos pronto, así que

por el bien de todos desiste de transmitir cualquier cosa hasta que el intercambio este completo. A partir de la información proporcionada en la solicitud RTS, *C* puede estimar cuanto tardará la secuencia, incluyendo el ACK final, por lo que impone para sí misma un tipo de canal virtual ocupado, indicado por **NAV (Vector de asignación de Red)** en la *figura 1.10*. *D* no escucha el RTS, pero si el CTS, por lo que también impone la señal *NAV* para sí misma. Observe que las señales *NAV* no se transmiten; simplemente son recordatorios internos para mantenerse en silencio durante cierto periodo.

En contraste con las redes cableadas, las inalámbricas son ruidosas e inestables, en gran parte debido a hornos de microondas, que también utilizan las bandas sin licencia ISM Industrial Scientific Medical. Como consecuencia, la probabilidad de que una trama llegue a su destino se decrementa con la longitud de la trama. Si la probabilidad de que cualquier bit sea erróneo es p, entonces la probabilidad de que una trama de n bits se reciba por completo y correctamente es $(1-p)^n$. Por ejemplo, para $p=10^{-4}$, la probabilidad de recibir correctamente una trama Ethernet completa (12,144bits) es menor que 30%. Si $p=10^{-5}$, aproximadamente una trama de 9 estará dañada. Incluso si $p=10^{-6}$, más de 1% de las tramas se dañará, lo que equivale a casi una docena por segundo y más si se utilizan tramas mas cortas que el máximo. En resumen, si una trama es demasiado grande, tiene muy pocas probabilidades de pasar sin daño y probablemente tenga que retransmitirse.

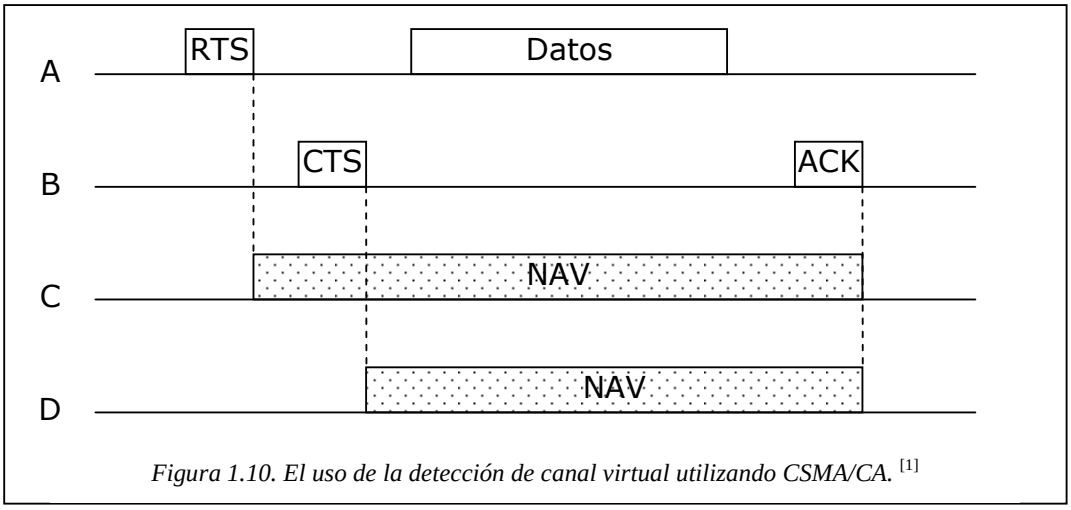


Figura 1.10. El uso de la detección de canal virtual utilizando CSMA/CA. [1]

Para solucionar el problema de los canales ruidosos, 802.11 permite dividir las tramas en fragmentos, cada uno con su propia suma de verificación. Cada fragmento se numera de manera individual y su recepción se confirma utilizando un protocolo de

parada y espera (es decir, el emisor podría no transmitir fragmentos de *k*+1 hasta que haya recibido la confirmación de recepción del fragmento *k*). Una vez que se ha adquirido el canal mediante RTS y CTS, pueden enviarse múltiples fragmentos en una fila, como se muestra en la *figura 1.11*. La secuencia de fragmentos se conoce como **ráfaga de fragmentos**.

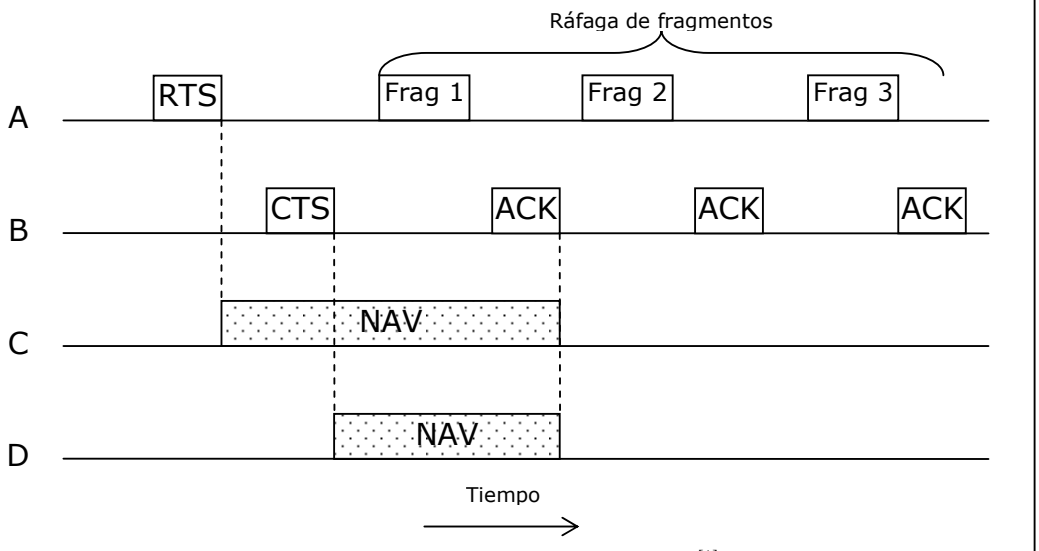


Figura 1.11. Una ráfaga de fragmentos. [1]

La fragmentación incrementa la velocidad real de transporte restringiendo las retransmisiones a los fragmentos erróneos en lugar de la trama completa. El tamaño del fragmento no lo fija el estándar pero es un parámetro de cada celda y la estación base puede ajustarlo. El mecanismo NAV mantiene otras estaciones en silencio sólo hasta la siguiente confirmación de recepción, pero se utiliza otro mecanismo (descrito a continuación) para permitir que otra ráfaga de fragmentos completa se envíe sin interferencia.

Todo el análisis anterior se aplica al modo DCF 802.11. En él, no hay control central y la estación compite por tiempo aire, como en Ethernet. El otro modo permitido es PCF, en el que la estación base sonde a las demás estaciones, preguntándoles si tienen tramas que enviar. Puesto que el orden de transmisión se controla por completo por la estación base en el modo PCF, no ocurren colisiones. El estándar prescribe el mecanismo para sondeo, pero no la frecuencia de sondeo, el orden de sondeo, ni el hecho de que las demás estaciones necesiten obtener un servicio igual.

El mecanismo básico consiste en que la estación base difunda una **trama beacon** (trama guía o faro) de manera periódica (de 10 a 100 veces por segundo). Esta trama contiene parámetros de sistema, como secuencias de salto y tiempos de permanencia (para FHSS), sincronización de reloj, etc. También invita a las nuevas estaciones a suscribirse al servicio de sondeo. Una vez que una estación se inscribe para el servicio de sondeo a cierta tasa, se le garantiza de manera efectiva cierta fracción de ancho de banda, y se hace posible proporcionar garantías de calidad de servicio.

La duración de la batería siempre es un problema de los dispositivos inalámbricos móviles, por lo que 802.11 pone atención al asunto de la administración de energía. En particular, una estación base puede conducir a una estación móvil al estado de hibernación hasta que dicha estación base o usuario la saquen de él de manera explícita. Sin embargo, el hecho de indicar a una estación que entre en estado de hibernación significa que la estación base tiene la responsabilidad de almacenar en el búfer de tramas que vayan dirigidas a ella mientras la estación móvil esté hibernando. Posteriormente, esas tramas pueden colectarse.

PCF y DCF pueden coexistir dentro de una celda. Al principio podría parecer imposible tener control central y distribuido funcionando al mismo tiempo, pero 802.11 proporciona una forma de analizar este objetivo. Funciona cuidadosamente en el intervalo de tiempo entre tramas. Después de que se ha enviado una trama, se necesita cierta cantidad de tiempo muerto antes de que cualquier estación pueda enviar una trama. Se definen cuatro intervalos diferentes, cada uno con propósito específico. Estos intervalos se describen en la *figura 1.12.*

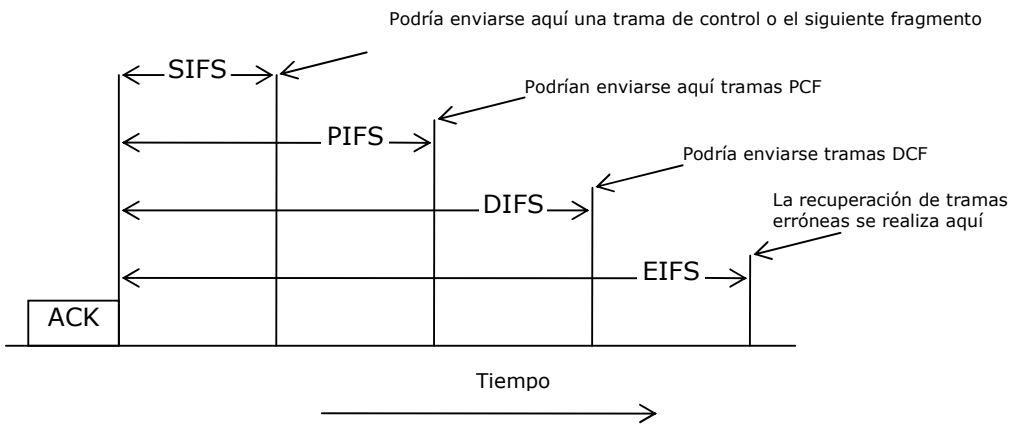


Figura 1.12. Espaciado entre tramas 802.11. [1]

El intervalo más corto es **SIFS (Espaciado Corto Entre Tramas)**. Se utiliza para permitir que las distintas partes de un diálogo transmitan primero. Eso incluye dejar que el receptor envíe un CTS para responder a una RTS, dejar que el receptor envíe un ACK para un fragmento o una trama con todos los datos y dejar que el emisor de una ráfaga de fragmentos transmita el siguiente fragmento sin tener que enviar una RTS nuevamente.

Siempre hay una estación que debe responder después de un intervalo SIFS. Si falla al utilizar su oportunidad y transcurre un tiempo **PIFS (Espaciado Entre Tramas PCF)**, la estación base podría enviar una trama de *beacon* o una trama de sondeo. Este mecanismo permite que una estación base envíe una trama de datos o una secuencia de fragmentos para finalizar su trama sin que nadie interfiera, pero le da a la estación base la oportunidad de tomar el canal cuando el emisor anterior haya terminado, sin tener que competir con usuarios ansiosos.

Si la estación base no tiene nada que decir y transcurre un tiempo **DIFS (Espaciado Entre Tramas DCF)**, cualquier estación podría intentar adquirir el canal para enviar una nueva trama. Se aplican las reglas de contención normales, y si ocurre una colisión, podría necesitarse el retroceso exponencial binario.

Sólo una estación que acaba de recibir una trama errónea o desconocida utiliza el último intervalo de tiempo, **EIFS (Espaciado Entre Tramas Extendido)**, para reportar la trama errónea. La idea de dar a este evento la menor prioridad es que debido a que el receptor tal vez no tenga idea de lo que está pasando, debe esperar un tiempo considerable para evitar interferir con un diálogo en curso entre las dos estaciones.

1.6.4. La pila de protocolos del 802.11. [1]

Los protocolos utilizados por todas las variantes de 802, entre ellas ethernet, tienen ciertas similitudes de estructura. En la *figura 1.13.* se muestra una vista parcial de la pila de protocolos del estándar 802.11. La capa física corresponde muy bien con la capa física OSI, pero la capa enlace de datos de todos los protocolos 802.11 se divide en 2 o más sub-capas. El estándar 802.11, la sub-capa MAC determina la forma en que se asigna el canal, es decir, a quien le toca transmitir a continuación. Arriba de dicha sub-capa se encuentra la sub-capa LLC, cuyo trabajo es ocultar las diferencias entre las variantes 802 con el propósito de que sean imperceptibles para la capa red. El estándar 802.11 de 1997 especifica tres técnicas de transmisión permitidas en la capa física.

El método de infrarrojos utiliza en su mayor parte la misma tecnología que los controles remotos de televisión. Los otros dos métodos utilizan el radio de corto alcance, mediante técnicas conocidas como FHSS Frecuency Hopping Spread Spectrum y DSSS Direct Secuense Spread Spectrum. Éstas utilizan parte del espectro que no necesita licencia (la banda ISM de 2,4GHz). Los abridores de puertas de cocheras controlados por radio también utilizan esta parte del espectro, por lo que su computadora portátil podría encontrarse compitiendo con la puerta de la cochera.

Los teléfonos inalámbricos y los hornos microondas también utilizan esta banda. Todas estas técnicas funcionan a 1 o 2 Mbps y con poca energía por lo que no interfieren mucho entre sí.

En 1999 se introdujeron dos nuevas técnicas para alcanzar un ancho de banda más alto. Éstas se conocen como OFDM Orthogonal Frecuency Division Multiplexing y HRDSSS Direct Secuense Spread Spectrum. Funcionan hasta 54 y 11 Mbps, respectivamente. En 2001 se introdujo una segunda modulación OFDM, pero en una banda de frecuencia diferente respecto a la primera.

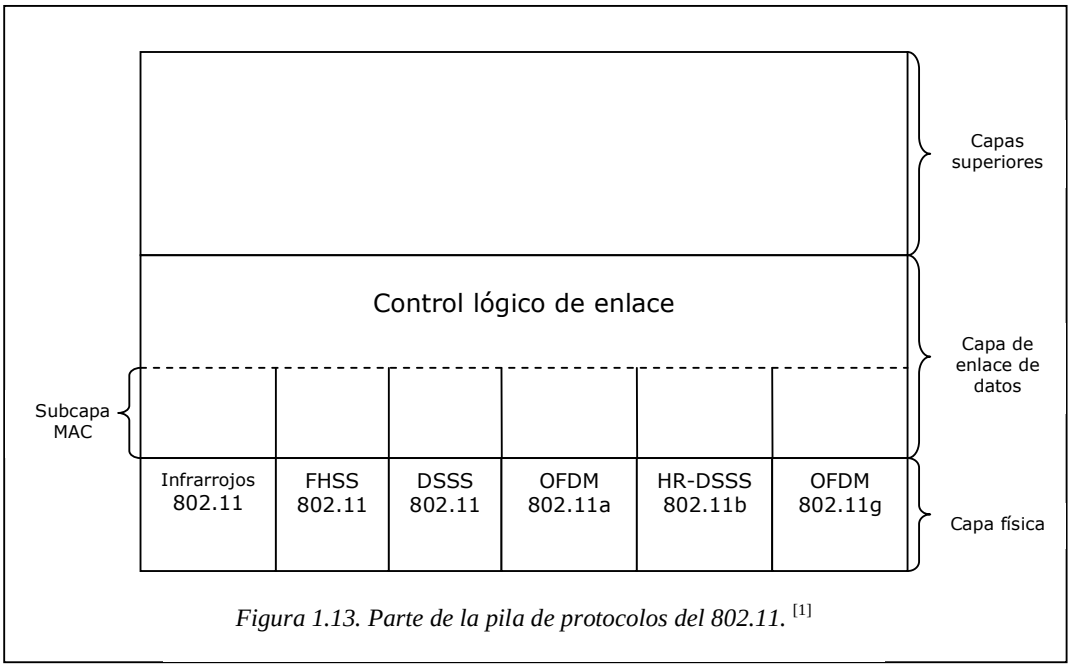


Figura 1.13. Parte de la pila de protocolos del 802.11. [1]

1.6.4.1. IEEE 802.11a. [4]

La especificación IEEE 802.11a hace uso de la banda de los 5GHz. Al contrario que en el caso de las especificaciones en la banda de los 2,4GHZ, en IEEE 802.11a no se emplea un esquema de espectro expandido, sino multiplexación por división de

frecuencia ortogonal (OFDM, Ortogonal Frecuenzy Division Multiplexing). OFDM, también conocido como modulación multiportadora, utiliza varias señales portadoras con frecuencias diferentes, enviando algunos de los bits totales por cada canal. Se trata de un esquema similar a FDM. Sin embargo, en el caso de OFDM todos los subcanales están dedicados a una única fuente de datos.

Las velocidades de datos posibles en IEEE 801.11a son 6, 9, 12, 18, 24, 36, 48, 54 Mbps. El sistema utiliza hasta 52 subportadoras que se modulan usando BPSK Binary Phase Shift Keying, QPSK Quadrature Phase Shift Keying, QAM-16 Quadrature Amplitude Modulation 16 bits, QAM-64 Quadrature Amplitude Modulation 64 bits, en función de la velocidad requerida. El espaciado entre frecuencias subportadoras es de 0,3125MHz. Un código convolucional a una tasa de 1/2, 2/3, o 3/4 proporciona corrección de errores hacia delante.

1.6.4.2. IEEE 802.11b. [4]

IEEE 802.11b es una extensión del esquema IEEE 802.11 DSSS, proporcionando velocidades de datos de 5,5 y 11 Mbps. La tasa de minibits es de 11MHz, la misma que el esquema DSSS original, proporcionando así el mismo ancho de banda ocupado. Para conseguir una velocidad de datos mayor en el mismo ancho de banda y con la misma tasa de minibits se utiliza un esquema de modulación conocido como modulación por código complementario (CCK, Complementary Code Keying).

El esquema de modulación CCK es bastante complejo y no será examinado aquí en detalle. La *figura 1.14.* Proporciona una idea general del esquema para una velocidad de datos de 11Mbps. Los datos de entrada son manejados en bloques de 8 bits a una tasa de 1,375MHz (8bits/símbolo*1,375MHz = 11Mbps). Seis de estos bits son transformados en una de las 64 secuencias de código. La salida de esta transformación, junto con los dos bits adicionales, constituye la entrada de un modulador QPSK.

1.6.4.3. IEEE 802.11g. [4]

IEEE 802.11g es una extensión de IEEE 802.11b a mayor velocidad. Este esquema combina toda una gama de técnicas de codificación del medio físico utilizadas en 802.11a y 802.11b para proporcionar servicio a diversas velocidades de datos.

IEEE 802.11g soporta tasas de transmisión de datos de 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1 Mbps.

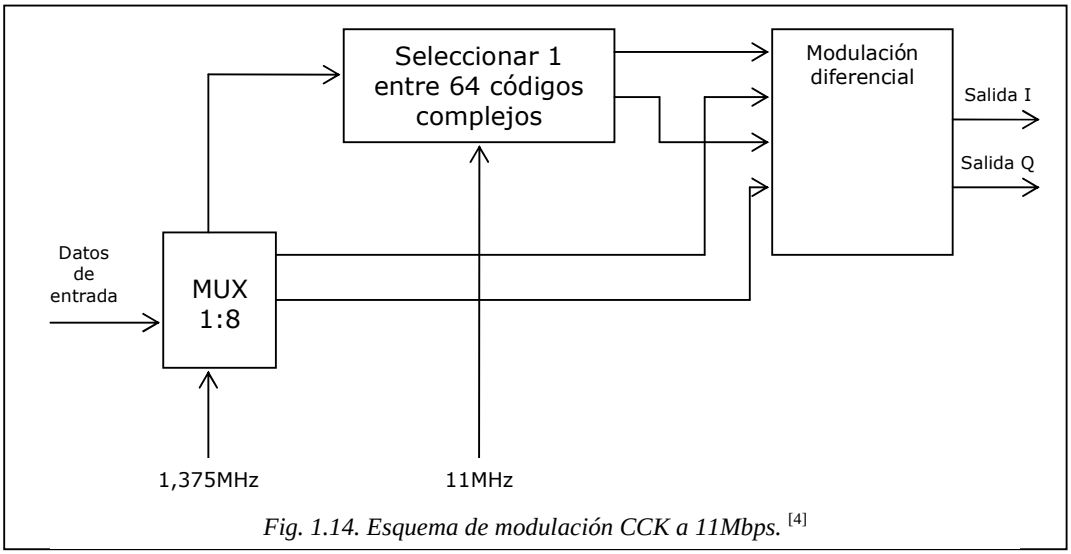


Fig. 1.14. Esquema de modulación CCK a 11Mbps. [4]

1.7. PRODUCTOS Y ESTÁNDARES DE LAS REDES INALÁMBRICAS.

1.7.1. Productos de las Redes Inalámbricas. [3]

Una gran cantidad de productos en el mundo soportan el estándar IEEE 802.11b para redes WLAN, mientras que las compañías europeas están produciendo dispositivos basados en el estándar HiperLan II. 802.11 ha estado en uso durante muchos años de una forma u otra.

El área de los estándares para WLAN, podemos comprobar que la seguridad se describe una y otra vez como una opción. Aunque se le presta la apropiada atención en todas las evaluaciones de redes WLAN, la seguridad se contempla, fundamentalmente, como un obstáculo para incrementar la velocidad de transmisión de datos, y sólo después se la considera como un mecanismo apropiado de protección. La responsabilidad de la seguridad se hace recaer claramente sobre el usuario, si bien las mejoras más recientes en los estándares incluyen algunos avances en el tema de seguridad.

1.7.1.1. "Access Point". [13]

En la gestión de redes de computadoras, un punto de acceso inalámbrico (AP) es un dispositivo que conecta los dispositivos de la comunicación por radio, para formar una red inalámbrica. El AP normalmente se conecta a una red cableada, y puede relevar los datos entre los dispositivos inalámbricos y los dispositivos cableados. Varios APs pueden unirse para formar una red más grande que permite "roaming" entre ellos. (En

contraste, una red dónde los dispositivos del cliente se manejan sin la necesidad de cualquier AP se vuelve una red ad-hoc) los APs Inalámbricos tienen las direcciones IP grabadas internamente para su configuración.

1.7.1.2. Tarjetas Inalámbricas. [12]

Una tarjeta interfase de red inalámbrica (WNIC Wireless Network Interfase Conection) es una tarjeta de red que conecta a una red de computadores, diferente a una tarjeta de red normal (NIC Network Interfase Conection) qué conecta a una red cableada o ethernet. Una WNIC, sólo como una NIC, trabaja en la Capa 1 y Capa 2 del Modelo OSI.

Una WNIC es un componente esencial para el ordenador inalámbrico. Esta tarjeta usa una antena para comunicar a través de las microondas. Una WNIC en un ordenador es principalmente localizado en la hendidura de PCI, PCMCIA o interna. Otras opciones son USB WNIC, WNIC PCMCIA y WNIC integrados.

Una WNIC puede operar en dos modos conocido como el modo de la infraestructura y el modo ad-hoc. Se diseñan WNICs de acuerdo al estándar IEEE 802.11.

1.7.1.3. Antenas. [5]

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas.

Aumentan la zona de influencia / cobertura de nuestros productos inalámbricos, de manera que en lugar de dar cobertura a unos pocos metros, podemos alcanzar cientos de metros sin problemas.

Básicamente encontramos dos tipos de antenas:

- Antenas Omnidireccionales
- Antenas Direccionales

Antenas Omnidireccionales

Cobertura con diagrama de radiación circular (360º).

Los diagramas son óvalos, debido a la cercanía con las frecuencias microondas.

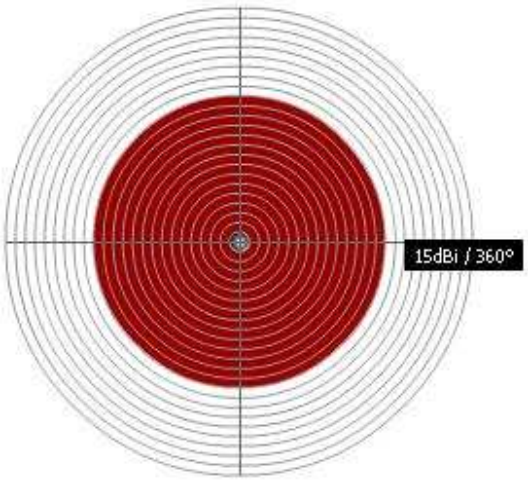


Figura 1.15. Diagrama de radiación de una Antena Omnidireccional. [5]

Antenas Direccionales

Patrón de radiación muy fuerte en dirección específica, focaliza radiación de la energía. Ej.: Antenas Yagi, Patch y Parabólica

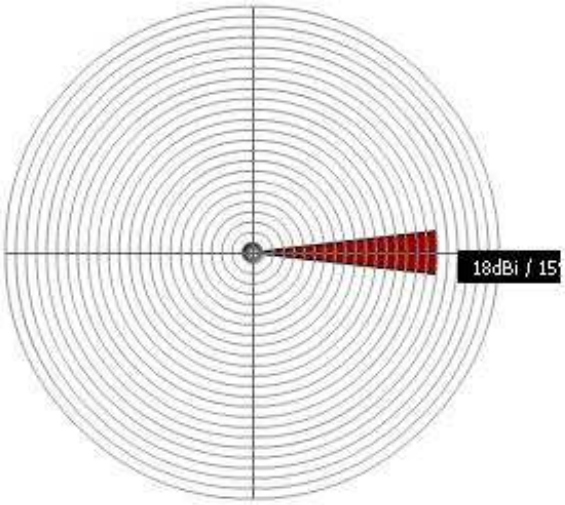


Figura 1.16. Diagrama de radiación de una Antena Direccional. [5]

1.7.2. Estándares de las Redes Inalámbricas. [2]

Se pueden distinguir principalmente los siguientes estándares relacionados con las redes inalámbricas (realmente, únicamente se puede considerar como estándar los dos primeros y los otros dos como tecnologías especializadas):

- **IEEE 802.11** que cubre *FHSS*, *DSSS* y tecnologías infrarrojas (las versiones radiofrecuencia se diseñaron para edificios de empresas con muchas oficinas o

construcciones de organizaciones con muchos edificios, con el fin de poder moverse libremente entre los distintos puntos de control inalámbricos que estén conectados a la red). Actualmente, se está ampliando con **802.11b** (una versión de transmisión de datos superior a 2,4GHz con *DSSS*), **802.11a** (una versión de transmisión de datos de 5GHz) y **802.11e** que abarca tanto los entornos de negocios como los domésticos y añade prestaciones de calidad de servicio y soporte multimedia a las actuales normas inalámbricas *802.11a* y *802.11b*, con las que es compatible. Teóricamente, la versión *802.11b* tiene un funcionamiento de 11Mbps equivalente al de Ethernet con cable (pero la realidad es distinta, ya que el rendimiento real se aproxima más a 5Mbps). Aun así, proporciona un importante adelanto en rapidez sobre las generaciones anteriores.

- **HiperLan.** El **ETSI (European Telecomunications Standards Institute)** llevó a cabo durante los años 1991 y 1996 este proyecto con el que pretendía conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11. Incluía cuatro estándares diferentes, de los cuales el denominado Tipo 1 es el que verdaderamente se ajusta a las necesidades futuras de las WLAN, estimándose una velocidad de transmisión de 23,5Mbps (54Mbps con HiperLan/2), muy superior a los 11Mbps de la actual normativa IEEE 802.11b.

- **Bluetooth** que es una tecnología de corto alcance y de bajo consumo diseñado para conexión de periféricos a computador o para dispositivos portátiles (por ejemplo, los auriculares inalámbricos de *Ericsson*. Como en Europa no está permitido conducir con un teléfono móvil, utilizando dichos auriculares y un teléfono *Bluetooth*, sólo es necesario decir *responder* o *llamar al número determinado* para realizar la conexión, aunque el teléfono se encuentre en un maletín o en una cartera). Está optimizada para los receptores de radio de bajo consumo ideales para los dispositivos personales. Su alcance reducido es bueno para detecciones de proximidad pero como las señales no son suficientemente fuertes para penetrar paredes, suelos o cubrir toda una casa, no es adecuado para redes inalámbricas.

- **HomeRF** que es una tecnología diseñada para la conectividad sin hilos dentro de un hogar e, incluso, interoperar con las redes públicas de telefonía e *Internet*.

Opera en la banda *ICM* de 2,4GHz, pero combinando elementos de los estándares **DECT (Digitally Enhanced Cordless Tlephone)** e *IEEE 802.11*.

1.7.2.1. El estándar IEEE 802.11. [2]

El fundamento de muchas de las actuales redes inalámbricas se encuentra basado en el estándar IEEE 802.11 y, más correctamente, en la nueva especificación IEEE 802.11b. Con este estándar se garantiza la interoperatividad entre fabricantes, consiguiendo al mismo tiempo una significativa reducción de costos y, consiguientemente, un abaratamiento de los dispositivos para el usuario final.

En 1990, en el seno del comité IEEE 802, se formo el IEEE 802.11, que empezó a trabajar para tratar de generar una norma para las WLAN. En 1994 apareció el primer borrador y hubo que esperar hasta junio de 1997 para dar por finalizada la norma.

En 1992 se creó **Winforum**, consorcio liderado por *Apple* y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencias para los sistemas *PCS (Personal Comunications Systems)*. En ese mismo año, la **ETSI (European Telecomunications Standards Institute),** a través de su comité ETSI-RES 10, inició distintas actuaciones para crear una norma a la que se denominó **HiperLan (High Performance LAN)** y asignarle (posteriormente) las bandas de 5,2 y 17,1 GHz.

En 1993 se constituyó la **IRDA (Infrared Data Association)** para promover el desarrollo de las **WLAN** basadas en enlaces por infrarrojos.

En 1996 un grupo de empresas del sector de informática móvil y de servicios forman el WLI Forum (Wirereless LAN Interoperability Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores se encuentran empresas como *Data General, Seiko, Epson y Zenith Data Systems.*

Finalmente, el consorcio WECA (Wireless Ethernet Compatibility Alliance), formado por un nutrido grupo de relevantes empresas, ha establecido un estándar llamado Wi-Fi que permite la certificación de los productos acogidos a esta normativa para lograr que entre ellas exista una obligada compatibilidad y otros aspectos comunes de actuación como la facilidad de configuración, unanimidad de protocolos, modos de funcionamiento y otros.

Arquitectura y Servicios de IEEE 802.11. [4]

En 1990 se formó IEEE 802.11 con el propósito de desarrollar un protocolo MAC y una especificación del medio físico para las redes LAN inalámbricas. La *tabla 1.1*. define brevemente los términos clave utilizados en el estándar IEEE 802.11.

Arquitectura de IEEE 802.11. [4]

En la *figura 1.17*. se ilustra el modelo desarrollado por el grupo de trabajo IEEE 802.11. El componente elemental de una red LAN Inalámbrica es un conjunto básico de servicios *(BSS, Basic Service Set)*, consistente en un número de estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. Un BSS puede funcionar aisladamente o bien estar conectado a un sistema troncal de distribución *(DS, Distribution System)* a través de un punto de acceso *(AP, Access Point)* que efectúa las funciones de puente. El protocolo MAC puede ser completamente distribuido o bien estar controlado por una función central de coordinación ubicada en el punto de acceso. Generalmente, el BSS se corresponde con lo que en la bibliografía es referido como "celda". Por otro lado, el DS puede ser un conmutador, una red cableada tradicional u otra red inalámbrica.

Punto de acceso (AP)	Cualquier entidad que tenga la funcionalidad de una estación y proporcione acceso al sistema de distribución a través del medio inalámbrico a las estaciones asociadas.
Conjunto básico de servicios (BSS)	Conjunto de estaciones controladas por una sola función de coordinación.
Función de coordinación	Función lógica que determina cuando una estación funcionando dentro de un BSS tiene permiso para transmitir y puede recibir PDU.
Sistema de distribución (DS)	Sistema utilizado para interconectar un conjunto de BSS y LAN integradas para crear un ESS.
Conjunto extendido de servicios (ESS)	Conjunto de uno o más BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC de cualquier estación asociada con uno de tales BSS.
Unidad de datos del	Unidad de datos intercambiada entre entidades MAC

protocolo MAC (MPDU)	paritarias usando los servicios de la capa física.
Unidad de datos del servicio MAC (MSDU)	Información entregada como una unidad entre usuarios MAC.
Estación	Cualquier dispositivo que contenga capas físicas y MAC compatibles con IEEE 802.11.

Tabla 1.1. Terminología IEEE 802.11. [4]

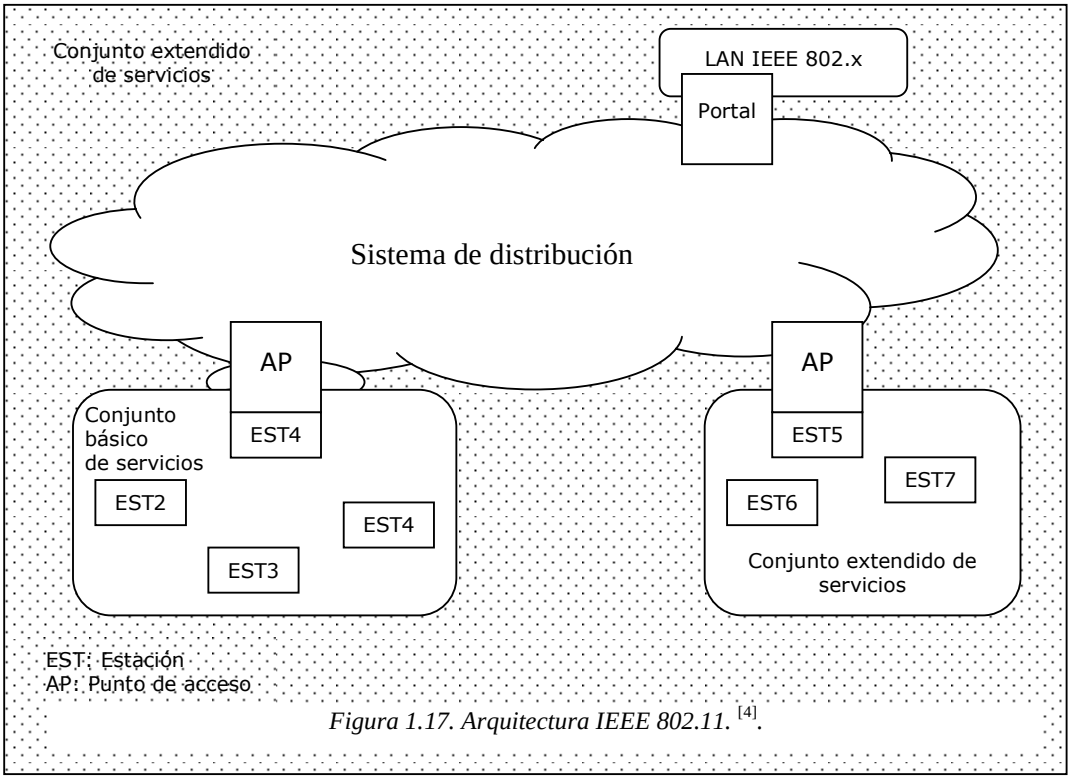


Figura 1.17. Arquitectura IEEE 802.11. [4].

La configuración más simple posible es la mostrada en la *figura 1.17.*, en la que cada estación pertenece a un BSS aislado; esto es, cada estación se encuentra dentro del rango de otras estaciones que pertenecen al mismo BSS. Es igualmente posible que exista un solapamiento geográfico entre dos BSS, de manera que una estación podría formar parte de más de un BSS. Además, la asociación entre una estación y un BSS es dinámica, puesto que una estación puede apagarse, salirse de la distancia máxima permitida o incorporarse de nuevo.

Un conjunto extendido de servicios (*ESS, Extended Service Set*) consiste en dos o más conjuntos básicos de servicios interconectados mediante un sistema de distribución. Este último es, por lo general, una LAN cableada troncal, aunque puede tratarse de

cualquier red de comunicaciones. El conjunto extendido de servicios aparece a nivel de control de enlace lógico (LLC) como una única red LAN lógica.

En la *figura 1.17.* se indica que un AP se implementa como parte de una estación. El AP constituye la lógica dentro de la estación que proporciona el acceso al DS a través de los servicios de distribución, además de servir como estación. La integración de una arquitectura 802.11 con una red LAN cableada tradicional se realiza a través de un portal. La lógica del portal se implementa en un elemento, como un puente o un dispositivo de encaminamiento, que forme parte de la LAN cableada y que se encuentre conectado al DS.

Servicios que presta el protocolo 802.11.

El estándar 802.11 afirma que cada LAN inalámbrica que se apegue a él debe proporcionar nueve servicios. Éstos se dividen en dos categorías: cinco servicios de distribución y cuatro de estación. Los servicios de distribución se relacionan con la administración de membresías dentro de la celda y con la interacción con estaciones que están fuera de la celda. En contraste, los servicios de estación se relacionan con la actividad dentro de una sola celda.

Los cinco servicios de distribución son proporcionados por la estación base y tienen que ver con la movilidad de la estación conforme entran y salen de las celdas conectándose ellos mismos a las estaciones base y separándose ellos mismo de dichas estaciones. Estos servicios son los siguientes:

1. **Asociación.** Este servicio es utilizado por las estaciones móviles para conectarse ellas mismas a las estaciones base. Por lo general, se utiliza después de que una estación se mueve dentro del alcance de radio de la estación base. Una vez que llega, anuncia su identidad y sus capacidades. Éstas incluyen las tasas de datos soportadas, necesarias para los servicios PCF (es decir, el sondeo), y los requerimientos de administración de energía. La estación base podría aceptar o rechazar la estación móvil. Si se acepta, dicha estación debe autenticarse.
2. **Disociación.** Es posible que la estación o la estación base se disocie, con lo que se rompería la relación. Una estación podría realizar este servicio antes de apagarse o de salir, pero la estación base también podría utilizarlo antes de su mantenimiento.

3. **Reasociación.** Una estación podría cambiar su estación base preferida mediante este servicio. Esta capacidad es útil para estaciones móviles que se mueven de una celda a otra. Si se utiliza correctamente, no se perderán datos como consecuencia del cambio de estación base (*handover*). (Pero 802.11, al igual que Ethernet, es sólo un servicio de mejor esfuerzo).
4. **Distribución.** Este servicio determina como enrutar tramas enviadas a la estación base. Si el destino es local para la estación base, las tramas pueden enviarse directamente a través del aire. De lo contrario, tendrán que reenviarse a través de la red cableada.
5. **Integración.** Si una trama necesita enviarse a través de una red no 802.11 con un esquema de direccionamiento o formato de trama diferentes, este servicio maneja la traducción del formato 802.11 al requerido por la red de destino.

Los cuatro servicios restantes son dentro de las celdas (es decir, se relacionan con acciones dentro de una sola celda). Se utilizan después de que ha ocurrido la asociación y son las siguientes:

6. **Autenticación.** Debido a que las estaciones no autorizadas pueden recibir o enviar con facilidad la comunicación inalámbrica, una estación debe autenticarse antes de que se le permita enviar datos. Una vez que la estación base asocia una estación móvil (es decir, la ha aceptado en su celda), le envía una trama especial de desafío para ver si dicha estación móvil sabe la clave secreta codificando la trama de desafío y regresándola a la estación base. Si el resultado es correcto, la estación móvil se vuelve miembro de la celda. En el estándar inicial, la estación base no tiene que probar su identidad a la estación móvil, pero se está realizando trabajo para reparar este defecto en el estándar.
7. **Desautenticación.** Cuando una estación previamente autenticada desea abandonar la red, se desauntentica. Después de esto, tal vez ya no utilice la red.
8. **Privacidad.** Para que la información que se envía a través de una LAN inalámbrica se mantenga confidencial, debe codificarse. Este servicio maneja la codificación y decodificación. El algoritmo de codificación especificado es RC4, inventado por Ronald Rivest del M.I.T.
9. **Entrega de datos.** Por último, la transmisión de datos es la parte esencial, por lo que el 802.11 naturalmente proporciona una forma de transmitir y recibir

datos. Puesto que el 802.11 está basado en Ethernet y no se garantiza que la transmisión a través de Ethernet sea 100% confiable, tampoco se garantiza que la transmisión a través de 802.11 sea confiable. Las capas superiores deben tratar con la detección y la corrección de errores.

Una celda 802.11 tiene algunos parámetros que pueden inspeccionarse y, en algunos casos, ajustarse. Se relacionan con la codificación, intervalos de expiración de temporizador, tasas de datos, frecuencia de la trama de *beacon*, etc.

Las LAN inalámbricas basadas en 802.11 se están comenzando a distribuir en edificios de oficinas, aeropuertos, hoteles, restaurantes y universidades de todo el mundo. Se espera un crecimiento rápido.

802.11	La WLAN estándar original. Soporta desde 1 Mbps hasta 2 Mbps.
802.11a	Estándar WLAN de alta velocidad para la banda de 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2,4 GHz. Soporta hasta 11 Mbps.
802.11d	Itinerancia internacional: configura dispositivos automáticamente para que cumplan con las regulaciones RT locales
802.11e	Dirige la calidad de los requisitos de servicios para todas las interfaces de radio de WLAN IEEE.
802.11f	Define comunicaciones del punto de acceso interno para facilitar redes WLAN múltiples distribuidas por proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de 2,4 GHz. Soporta velocidades de hasta 54 Mbps.
802.11h	Define la gestión del espectro de la banda de 5 GHz.
802.11i	Dirige las flaquezas de la seguridad actual tanto para los protocolos de codificación como de autenticación. El estándar abarca los protocolos 802.1X, TKIP y AES.
802.11n	Proporciona mejoras de mayor capacidad de proceso. Se pretende que proporcione velocidades de hasta 500 Mbps.

Tabla 1.2. Estándares 802.11. [10]

1.8. SEGURIDADES EN LAS REDES INALÁMBRICAS. [10]

Un problema de la tecnología inalámbrica es la seguridad. Sin ninguna restricción debido a la ausencia de limitaciones físicas de los cables y las paredes, las WLAN han demostrado ser delicadas en cuestión de seguridad. Los piratas informáticos rompían fácilmente estos esfuerzos iniciales debido a la protección equiparable a la de redes cableadas (WEP), uno los primeros protocolos de seguridad. Esto produjo dudas en algunas empresas a la hora de adoptar la tecnología inalámbrica por miedo a que se pudieran interceptar y decodificar los datos transmitidos entre un dispositivo inalámbrico y un punto de acceso.

Para reforzar un modelo de seguridad, la alianza Wi-Fi introdujo su propia solución provisional de la especificación de seguridad de 802.11i: el acceso Wi-Fi protegido (WPA). WPA combinaba varias tecnologías para afrontar todas las vulnerabilidades de seguridad de 802.11. Proporcionaba una fuerte autenticación basada en el usuario mediante el uso del estándar 802.1X (un marco de autenticación mutuo diseñado para proporcionar un acceso de puerto controlado entre los dispositivos de cliente inalámbricos, los puntos de acceso y los servidores) y el EAP (protocolo de autenticación extensible). WPA también contaba con una sólida codificación mediante claves de codificación de 128 bits y el uso del protocolo TKIP (protocolo para la integridad de claves temporales). Un mensaje MIC (comprobación de la integridad del mensaje) evitaba que los piratas informáticos capturaran y alteraran o falsificaran los paquetes de datos. Esta combinación de tecnologías protegía la confidencialidad y la integridad de las transmisiones WLAN al tiempo que permitía garantizar que sólo los usuarios autorizados obtendrían acceso a la red. La mejora posterior de WPA en seguridad y facilidad de gestión ofrece distribución automática fundamental, claves maestras únicas para cada usuario y sesión y claves de codificación únicas por paquete.

El estándar IEEE, 802.11i, ratificado en junio de 2004 incorpora muchas de estas características ya en práctica mediante WPA. Algunos de los cambios sustanciales de 802.11i sobre WPA implican mejor codificación y transferencia. El estándar 802.11i también ofrece caché esencial para permitir la reconexión rápida con servidores cuando una persona vuelva. Y lo que es más, proporciona autenticación previa para una itinerancia rápida entre los puntos de acceso de la red.

El resultado final práctico de la ratificación de 802.11i es que el mercado de la tecnología inalámbrica debe explotar de nuevo ya que el firmware se actualiza y hay nuevos productos que entran en el mercado. Con 802.11i, toda la cadena de seguridad para la conexión, intercambio de credenciales, autenticación y codificación se vuelve mucho más sólida y eficaz en la protección frente a ataques dirigidos y no dirigidos. Ahora la red y la integridad de sesión sólo tienen que gestionarse y no protegerse.

1.8.1. Términos de Seguridad WLAN. [1]

Se utilizan varios estándares y protocolos de seguridad en la industria de la WLAN. Algunas definiciones comprenden importantes interdependencias entre unos y otros.

- **802.11 del IEEE:** La familia de estándares del Instituto de Ingeniería Eléctrica y Electrónica (IEEE) para las redes WLAN, la cual fue por primera vez introducido en 1997. El 802.11b es un estándar endosado y bajo registro de marca Wi-Fi por la Alianza Wi-Fi.
- **802.1x del IEEE:** Un estándar de seguridad que se caracteriza por tener una estructura de autenticación basada en puerto y una distribución dinámica de llaves de sesión para encriptación WEP. Se requiere de un servidor RADIUS.
- **802.11i del IEEE:** Un estándar de seguridad que el IEEE está actualmente desarrollando; se caracteriza por las protecciones de autenticación 802.1X y agrega el estándar de encriptación de avance (AES Advanced Encryption Standard) para la protección de encriptación junto a otras mejoras.
- **WPA:** El Acceso Protegido Wi-Fi (WPA) es un estándar de seguridad de la Alianza Wi-Fi que resuelve los inconvenientes de la encriptación de la Privacidad Equivalente Cableada (WEP), utilizando el Protocolo de Integridad de Llave temporal (TKIP), el cual se envuelve alrededor de la WEP y cierra sus hoyos de seguridad. El Acceso Protegido Wi-Fi (WPA), incluye además los beneficios de autenticación del estándar 802.1X.
- **EAP2:** El Protocolo de Autenticación Extensible (EAP) es un protocolo punto a punto que soporta métodos de autenticación múltiples. El soporte para los tipos de EAP depende del OS que se soporta.
- **TKIP:** El Protocolo de Integridad de Llave Temporal es utilizado por los estándares 802.1X y WPA para autenticar. Diseñado por los mejores

criptógrafos ofrece un recubrimiento alrededor de la WEP, cerrando los hoyos de seguridad de la misma.

- **WEP:** La Privacidad Equivalente Cableada (WEP) es el protocolo de seguridad 802.11 original para las redes inalámbricas.
- **VPN3:** La Tecnología de la Red Privada Virtual (VPN) ofrece protección WLAN adicional importante para datos críticos. La red privada virtual (VPN) protege una WLAN creando un túnel que resguarda los datos del mundo exterior.
- **RADIUS4:** El Servicio al Usuario de Marcado de Autenticación Remota (RADIUS) es un servidor de punto final que desempeña la autenticación utilizando el Protocolo de Autenticación Extensible (EAP). Este es un requerimiento del estándar de seguridad 802.1X del IEEE.

1.8.2. WEP, WPA y WPA2. [9]

La seguridad es un aspecto que cobra especial relevancia cuando se habla de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección no confiable. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN.

El problema de 802.11i está siendo su tardanza en salir al mercado. Su aprobación se dio en junio de 2004. Algunas empresas en vistas de que WEP (de 1999) era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como son las VPNs Virtual Private Network, para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN.

No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi decidió lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. El resultado, en 2003, fue WPA.

1.8.3. WEP. [9]

Características y funcionamiento.

WEP (*Wired Equivalent Privacy*, privacidad equivalente a cableada) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico

cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero se sabe ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Se observa que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena la clave secreta a continuación del IV formado el *seed*.
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed*, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *keystream.* Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32 Control de Redundancia Cíclica). A continuación se comprobará que el CRC-32 es correcto.

Cifrado WEP. [7]

Para el cifrado de los datos inalámbricos, el estándar 802.11 original definió la privacidad equivalente por cable (WEP). Debido a la naturaleza de las redes inalámbricas, la protección del acceso físico a la red resulta difícil. A diferencia de una red con cables donde se requiere una conexión física directa, cabe la posibilidad de que cualquier usuario dentro del alcance de un punto de acceso inalámbrico o un cliente inalámbrico pueda enviar y recibir tramas, así como escuchar otras tramas que se

envían, con lo que la interceptación y el espionaje remoto de tramas de red inalámbrica resultan muy sencillos.

WEP utiliza una clave compartida y secreta para cifrar los datos del nodo emisor. El nodo receptor utiliza la misma clave WEP para descifrar los datos. Para el modo de infraestructura, la clave WEP debe estar configurada en el punto de acceso inalámbrico y en todos los clientes inalámbricos. Para el modo ad hoc, la clave WEP debe estar configurada en todos los clientes inalámbricos.

Tal como se especifica en los estándares de IEEE 802.11, WEP utiliza una clave secreta de 40 bits. La mayor parte del hardware inalámbrico para IEEE 802.11 también admite el uso de una clave WEP de 104 bits. Si su hardware admite ambas, es mejor utilizar una clave de 104 bits.

Nota Algunos proveedores de productos inalámbricos anuncian el uso de una clave de cifrado inalámbrico de 128 bits. Es la suma de una clave WEP de 104 bits y otro número empleado durante el proceso de cifrado denominado vector de inicialización (un número de 24 bits). Asimismo, algunos puntos de acceso inalámbricos recientes admiten el uso de una clave de cifrado inalámbrico de 152 bits. Se trata de una clave WEP de 128 bits sumada al vector de inicialización de 24 bits.

Elección de una clave WEP.

La clave WEP debe ser una secuencia aleatoria de caracteres de teclado (letras mayúsculas y minúsculas, números y signos de puntuación) o dígitos hexadecimales (números del 0 al 9 y letras de la A a la F). Cuanto más aleatoria sea la clave WEP, más seguro será su uso.

Una clave WEP basada en una palabra (como un nombre de compañía en el caso de una pequeña empresa o el apellido si se trata de una red doméstica) o en una frase fácil de recordar se puede averiguar fácilmente. Después de que el usuario malintencionado haya determinado la clave WEP, puede descifrar las tramas cifradas con WEP, cifrar tramas WEP correctamente y comenzar a atacar la red. Aunque la clave WEP sea aleatoria, todavía se puede averiguar si se recopila y analiza una gran cantidad de datos cifrados con la misma clave. Por lo tanto, se recomienda cambiar la clave WEP por una nueva secuencia aleatoria periódicamente, por ejemplo, cada tres meses.

1.8.4. WPA. [9]

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publica en la norma IEEE 802.11i. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente madura y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP *(Extensible Authentication Protocol)* y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

- **EAP**. EAP, definido en la RFC 2284 *(Request for Comments)* es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*).
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

Mejoras de WPA respecto a WEP.

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

Modos de funcionamiento de WPA.

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente**. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **Con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

Cifrado WPA. [7]

IEEE 802.11i es un nuevo estándar que especifica mejoras en la seguridad de las redes locales inalámbricas. El estándar 802.11i soluciona muchos de los problemas de seguridad del estándar 802.11 original. Mientras se ratifica el nuevo estándar IEEE 802.11i, los proveedores de productos inalámbricos han acordado un estándar intermedio interoperable denominado WPA (acceso protegido Wi-Fi).

Con WPA, el cifrado se realiza mediante TKIP (Protocolo de integridad de claves temporales), que reemplaza WEP por un algoritmo de cifrado más seguro. A diferencia de WEP, TKIP proporciona la determinación de una única clave de cifrado de unidifusión de inicio para cada autenticación y el cambio sincronizado de la clave de cifrado de unidifusión para cada trama. Debido a que las claves TKIP se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA.

1.8.5. WPA2 (IEEE 802.11i). [9]

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este

aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS (Basic Service Set), sino también para el modo IBSS (Independent Basic Service Set) (redes ad-hoc).

Cifrado WPA2. [7]

WPA2™ es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar 802.11i. WPA2 admite las características de seguridad obligatorias adicionales del estándar 802.11i que no están incluidos para productos que admitan WPA. Con WPA2, el cifrado se realiza mediante AES (estándar de cifrado avanzado), que también reemplaza WEP por un algoritmo de cifrado más seguro. Al igual que TKIP para WPA, AES proporciona la determinación de una clave de cifrado de unidifusión de inicio exclusiva para cada autenticación y el cambio sincronizado de la clave de cifrado de unidifusión para cada trama. Debido a que las claves AES se determinan automáticamente, no es necesario configurar una clave de cifrado para WPA2. WPA2 es la forma más eficaz de seguridad inalámbrica.

CAPÍTULO 2.

DETERMINACIÓN DE NECESIDADES DE INTERCONECTIVIDAD PARA LA RED INALÁMBRICA.

2.1. DETERMINACIÓN DEL ÁREA DE CONECTIVIDAD DE LA RED INALÁMBRICA.

En la Escuela de Formación Tecnológica de la Escuela Politécnica Nacional, en el área de las oficinas de profesores no existe conexión a Internet.

En estas oficinas están ubicados alrededor de unos 13 profesores. Dichas oficinas de alguna forma están dotadas de una conexión bastante limitada a la red cableada de datos de la Politécnica a través de unos dos o tres puntos de acceso (cajetines RJ45).

De acuerdo a una inspección que se realizó con el fin de encontrar una solución a esta necesidad de conexión de varios profesores que actualmente no están gozando de los servicios que presta la red de datos de la Politécnica, se concluyó que la mejor solución a dicha necesidad es la implementación de un "Access Point" para proveer la conexión de varios usuarios a la red de la Politécnica.

En la inspección realizada se tomo en cuenta varios aspectos importantes para determinar la solución más fiable, económica y rápida de implementar, que se pueda llevar a cabo con los recursos existentes en el mercado moderno además aplicando los conocimientos adquiridos en la formación en la Escuela Politécnica Nacional.

Los aspectos que nos llevaron a escoger esta solución como la mejor son los siguientes:

- Una de las ventajas de las redes inalámbricas es la **flexibilidad,** en este caso se necesitó expandir la red cableada existente de la Politécnica para proveer de conectividad a varios usuarios, en este caso aproximadamente de 8 a 10 usuarios, por lo que, la implementación de un "Access Point" es la mejor opción para solventar está necesidad.
- Otra de las ventajas de las redes inalámbricas es la **facilidad de instalación**, en este caso nos es de mucha ventaja el no tener que modificar la infraestructura de las oficinas ya que la edificación es bastante antigua, difícil para realizar los trabajos de arquitectura que implica una red

cableada, con la implementación de dicho “Access Point” no será necesario más que la implementación de un punto de conexión eléctrica y un cable de datos desde un punto de red ubicado estratégicamente en una de las oficinas.

- Otro de los aspectos se refiere a una ventaja de las redes inalámbricas denominado como **costos de propiedad reducido**, dicho de otra forma, bajo costo de implementación; según los puntos mencionados anteriormente, considerando la flexibilidad para la expansión de la red se puede decir que es muy bajo el costo al utilizar un solo dispositivo “Access Point” para proveer de conexión a una gran cantidad de usuarios, que comparado con el alto costo que implicaría la implementación de un rack (de pequeñas dimensiones en este caso), switch, patch panel, cajetines, cable UTP, patch cords, canaletas, etc…, no hay comparación y definitivamente se elige una red inalámbrica por el bajo costo del “Access Point” frente al costo de todos los materiales sumados para una red cableada. Además, se puede acotar que actualmente en el creciente mercado de la tecnología inalámbrica se han reducido los costos de estos dispositivos inalámbricos. Por otra parte y haciendo referencia a la facilidad de instalación de una red inalámbrica, podemos decir que al no tener que hacer modificaciones en la infraestructura existente es obvio que el costo de instalación es más bajo, además, y por el mismo motivo, se lo implementaría en menor tiempo y se dispondría de menor mano de obra, lo que traducimos en bajos costos de instalación.

Según los puntos analizados anteriormente podemos concluir que la solución más fiable a esta necesidad es la implementación de un “Access Point” para proveer de conectividad a los usuarios que actualmente requieren de conexión a la red de la Politécnica.

2.2. CARACTERÍSTICAS DEL “ACCESS POINT”.

Según las necesidades planteadas para la implementación de esta red inalámbrica, se ha determinado las posibles características que debe cumplir el “Access Point” para poder proveer el servicio adecuado de conexión a los usuarios.

Entre las principales características se ha tomado en cuenta los siguientes aspectos:

- Como punto inicial se parte del objetivo del proyecto, debe cumplir con el principal objetivo que es de proveer de conexión como mínimo a unos 8 a 10 usuarios.
- El área en la que se va a implementar la red inalámbrica es de aproximadamente 35m de largo por unos 10m de ancho, por lo que, el equipo debe cubrir un área de aproximadamente $350m^2$, en la inspección realizada se tomo medidas aproximadas; la oficina 3 tiene 18m de largo por 10m de ancho, la oficina 4 tiene 10m de largo por 10m de ancho, entre las 2 oficinas hay un callejón de 4m de ancho por 10m de largo; en la *figura 2.1.* se ilustra estas medidas tomadas.
- Debe tener una potencia de señal en la antena que no se debilite fácilmente cuando pase por paredes bastante gruesas; en este caso la edificación es bastante antigua y la paredes bastante anchas de ladrillo, por lo que, el "Access Point" que se escoja deberá pasar esta prueba.
- Un aspecto muy importante es la compatibilidad, por lo que el equipo a escoger debe cumplir con los estándares que estén en vigencia actualmente, en este caso deberá cumplir con los estándares IEEE 802.11b para trabajar en la banda de 2.4GHZ y transmitir datos hasta 11Mbps, y IEEE 802.11g para trabajar en la banda de 2.4GHZ y transmitir datos hasta 54Mbps, que son los más usados en los equipos modernos. Además deberá tener conexión cableada (puerto RJ-45), que como mínimo deberá trabajar a la velocidad a la que trabaje actualmente la red de la EPN, en este caso según la investigación realizada la red de la EPN trabaja a 100Mbps, por lo que, dicho puerto en el "Access Point" debe trabajar a esta velocidad.
- Según las especificaciones de ampliación de red en la EPN, la administración de la red de datos de la EPN proveerá de una IP fija para el "Access Point", pero no para cada usuario, por lo que, el dispositivo que se escoja deberá tener la capacidad de proveer de IPs dinámicas, es decir, aparte de ser "Access Point" deberá ser Swith y Router.
- Por último y es un aspecto muy importante para la decisión final será el costo y la marca, se tomará en cuenta que la marca sea confiable, conocida y de preferencia certificada, y sobre el precio, se tomará en cuenta un equipo de mediano costo.

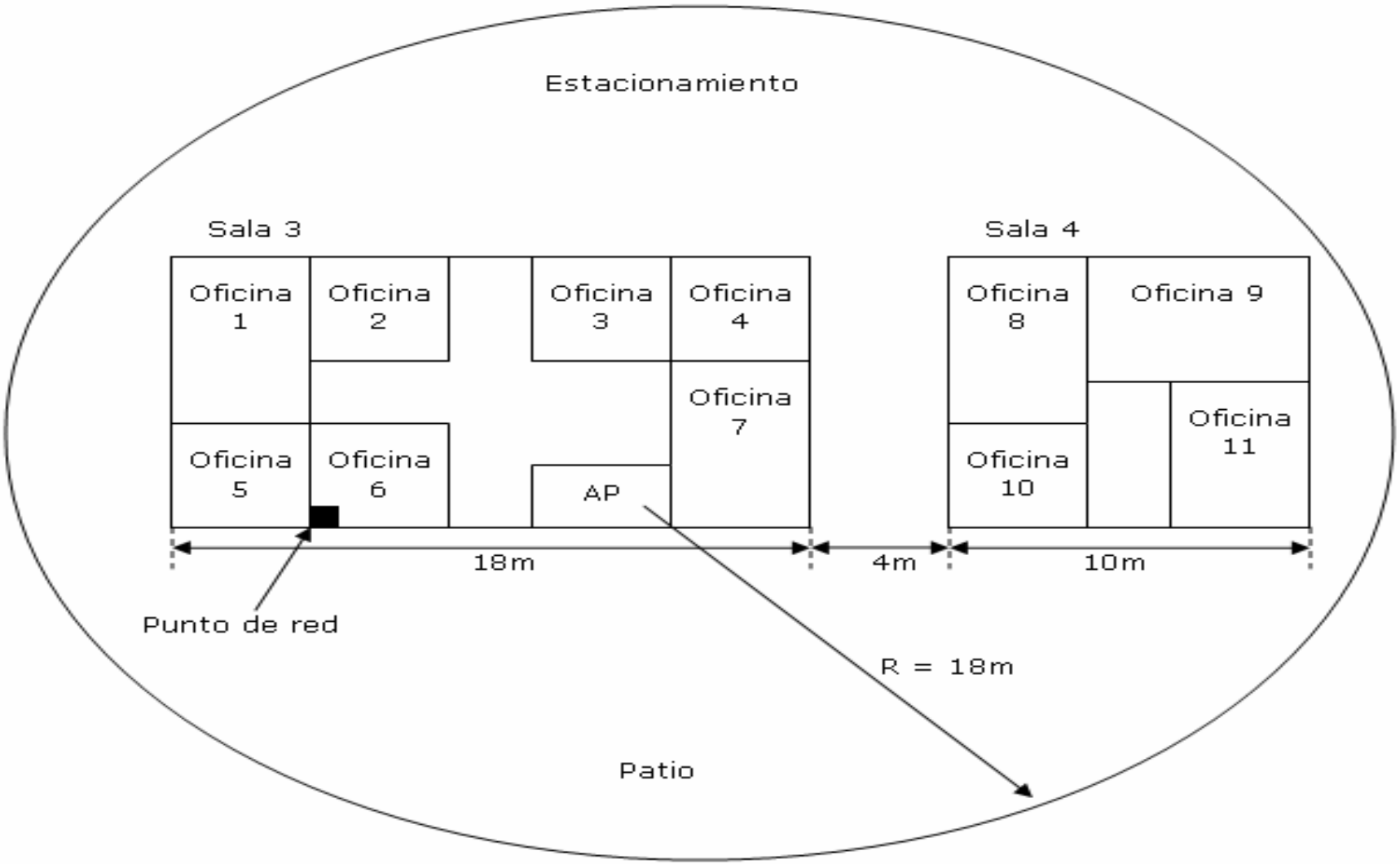


Figura 2.1. Plano de las Salas 3 y 4 de Profesores de la ESFOT

2.3. CONECTIVIDAD CON LA LAN DE LA EPN.

En este punto se hace una descripción del lugar en donde se implementará la red inalámbrica, tomando en cuenta aspectos como la ubicación física, forma y medidas del área en cuestión y algunos detalles de la estructura física de los edificios u oficinas ubicados en esta área. Para lo cual se ilustra en la *figura 2.1.* varios detalles importantes que influyen en la implementación del proyecto.

Según las inspecciones realizadas en las instalaciones donde se va a implementar la red inalámbrica, se encontró varias características de la estructura o edificación existente, característica que influyen para la elección de los equipos y material a utilizarse en la implementación.

El área correspondiente a las salas 3 y 4 de profesores de la ESFOT está ubicada en la parte norte del "CAMPUS" de la EPN, esta área está compuesta por varias edificaciones, todos son edificios muy antiguos y de paredes gruesas, en estas áreas están funcionando actualmente varias oficinas de profesores, aulas y laboratorios, cabe anotar que estos edificios internamente han sido adecuados con estructuras y modulares propios para oficinas, aulas y laboratorios; con el fin de brindar a los profesores y estudiantes instalaciones cómodas y adecuadas para el perfecto funcionamiento docente de la Institución.

En esta área donde funcionan varias oficinas de profesores ya se ha implementado algún tipo de conexión a la red de la EPN, algunas de ellas vía red cableada y otra vía inalámbrica. En la inspección realizada en las salas 3 y 4, se observó que hay varios puntos de red cableada en algunas oficinas dentro de estas salas, pero no en todas. Si el objetivo del proyecto es implementar una solución para proveer conexión a la red de la EPN a todos los profesores que laboran en esta área, implicaría poner tantos puntos como oficinas existen en dichas salas, claro que si la solución fuera una red cableada. Para este caso no interesa cuantos puntos de red cableada existen, solo nos interesa uno que es donde conectaremos el "Access Point", en la *figura 2.1.* se detalla la ubicación del punto de red y de "Access Point".

Según la administración de la red de la EPN se tendría un punto de red disponible para conectar el "Access Point", punto ubicado en una de las oficinas de la sala 3 de profesores, donde estará ubicado el "Access Point". Se necesitará también una

conexión a una toma eléctrica, hay varios “toma corrientes” eléctricos, y no hay dificultad en hacer una extensión para el “Access Point”.

Según lo expuesto en este punto se concluye que la conectividad con la red de la EPN es fácilmente implementable ya tomando en cuenta los recursos y estructura con la que contamos.

2.4. CARACTERÍSTICAS DE LA TARJETA INALÁMBRICA.

Este proyecto trata sobre la implementación de una red inalámbrica en general, lo que implica que existirá en este caso un emisor y varios receptores. El emisor viene a ser el “Access Point” que emitirá una señal con la que proveerá de varios servicios a los usuarios receptores. Los receptores o usuarios vienen a ser los equipos de cómputo utilizados para realizar varias tareas, una de ellas es la conexión a la red de la EPN, y una vez conectados a la red, hacer uso de servicios como Internet, Correo Electrónico, Base de Datos, etc.

Las características del dispositivo emisor “Access Point” ya se ha detallado anteriormente, por lo que, ahora se detalla las características de las tarjetas inalámbricas que deben tener los equipos de computo que se van a conectar a la red de la EPN por medio del “Access Point” a implementarse.

Los equipos de computo pueden ser de dos tipos: laptops o desktops. Por lo que, también tendremos dos tipos de tarjetas inalámbricas: una de tipo PCMCIA para laptops y una de tipo PCI para desktops, además en la actualidad se optado por utilizar tarjetas inalámbricas USB que sirven para cualquiera de los dos tipos de equipos que mencionamos, solo basta que el equipo tenga puertos USB, es decir, se tiene tres tipos de tarjetas inalámbricas.

Se ha mencionado tres tipos de tarjetas inalámbricas, según el tipo de equipo en el que se la va a instalar.

Ahora se hace referencia a varios aspectos que deben cumplir:

- Como primer aspecto debemos mencionar que la tarjeta debe cumplir con los estándares 802.11b y 802.11g, primero porque es el estándar que debe cumplir el “Access Point”; y como segunda razón podemos decir que es un estándar que los fabricantes actualmente han incorporado en algunos equipos de cómputo como en los laptops y en algunos desktops. Según los estándares mencionados que

deben soportar las tarjetas inalámbricas y que se mencionó en el Capítulo 2.2 que debe cumplir el “Access Point”, las tarjetas deben cumplir con IEEE 802.11b para trabajar en la banda de 2.4GHZ y transmitir datos hasta 11Mbps, y con IEEE 802.11g para trabajar en la banda de 2.4GHZ y transmitir datos hasta 54Mbps.

- También se ha tomado en cuenta los costos de las tarjetas, actualmente las tarjetas inalámbricas las hay de varios costos, pero cabe decir que han bajado los costos notablemente con el crecimiento del mercado de las redes inalámbricas, a tal punto que algunas ya se comparan con tarjetas de red para red cableada.

CAPÍTULO 3.

DETERMINACIÓN DEL EQUIPO Y CONFIGURACIÓN.

3.1. CARACTERÍSTICAS TÉCNICAS DE EQUIPOS.

En este punto se hace una lista de productos de la que se escoge el apropiado para la implementación del proyecto.

Se ha investigado el mercado de los productos inalámbricos y se ha escogido los productos de más aceptación en el mercado, para lo que se ha resumido en la *tabla 3.1*. productos de diferentes marcas de "Aceess Point".

3.1.1. Especificaciones de los "Access Point".

	C-Net	**Linksys**	**D-Link**
Nombre del Producto	Wireless-G Access Point	Wireless-G Broadband Router	AirPlusExtreme G
Modelo	CWA-854	WRT54G	DI-624
Características Principales	Switch y Access Point	Switch, Access Point y Router	Switch, Access Point y Router
Estándares	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b	IEEE 802.3, IEEE 802.3u, IEEE 802.3X, IEEE 802.11b, IEEE 802.11g	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Canales	11 Canales (US, Canada) 13 Canales (Europe and Japan)	1-11 canales (U.S.), 1-13 canales (Elsewhere Worldwide), 1-13,14 canales (Japan)	11 Canales (US, Canada) 13 Canales (Europe and Japan)
Puertos	Internet: Un puerto 10/100 RJ-45 LAN: cuatro 10/100 RJ-45 puertos Switcheados.	Un puerto 10/100 BaseT con conector RJ-45.	LAN: cuatro 10/100 RJ-45 puertos Switcheados.
Tipo de Cable	UTP CAT 5 o mejor	UTP CAT 5 o mejor	UTP CAT 5 o mejor
LEDs	Power, DMZ, WLAN, LAN (1, 2, 3, 4), Internet	Power (Verde), Link (Verde), WLAN (Verde)	Power, LAN (10/100), WLAN (Wireles connection)
Velocidad de transmisión	Wireless-G (802.11g a 54Mbps) y Wireless-B (802.11b a 11Mbps)	IEEE 802.11b: 1,2,5.5,11 Mbps; IEEE 802.11g: 6,9,12,18,24,36,48 y 54 Mbps; Ethernet: 10/100 Mbps	108Mbps, 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, 1Mbps

Dimensiones	W x H x D: 7.32" x 1.89" x 7.87"; (186 mm x 48 mm x 200 mm)	L x W x H: 129.5 x 78.5 x 26.7 mm (5.1" x 3.1" x 1.05")	L = 7.5 pulgadas (190.5mm), W = 4.6 pulgadas (116.84mm), H = 1.375 pulgadas (35mm)
Seguridad	Wi-Fi Protected Access™2 (WPA2), WEP, Wireless MAC Filtering	Hardware basado en IEEE 802.11i encriptado y desencriptado, incluye WEP 64bit y 128bit, TKIP y AES	64/128-WEP, 802.1X, WPA EAP, WPA PSK
Antena	2 Antenas externas desmontables	2 Antenas externas desmontables	1 Antena desmontable simple
Potencia de Salida RF	18 dBm	IEEE 802.11b: 17dBm y IEEE 802.11g: 13dBm	Para 802.11b con 1Mbps, 2Mbps, 5.5Mbps, 11Mbps: 18dBm. Para 802.11g con 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps: 18dBm y con 48Mbps, 54Mbps: 17dBm
Fuente de Poder	Externo, 12V DC, 0.5A	Externo, 5V DC, 2.5A	Externo, DC 5V, 2.4A
Costo	~ $105	~ $85	~ $110

Tabla 3.1. Características Comparativas de Productos

3.1.2. Especificaciones de la Tarjeta Inalámbrica.

Para establecer la solución se realizó pruebas de funcionamiento con un "Access Point" como emisor de señal, y un computador de tipo laptop con tarjeta inalámbrica integrada como receptor de señal. En la actualidad la mayoría de equipos laptops vienen con tarjeta inalámbrica integrada, por lo que fue de gran ayuda conseguir un equipo laptop para realizar las pruebas. Las características de la tarjeta inalámbrica usada para las pruebas de funcionamiento son las siguientes:

Fabricante	Intel
Modelo	Intel ® PRO Wireless 2200BG Network Conections
Tipo	Interna con antena en la pantalla.
Estándares y Velocidad	Trabaja con el estándar IEEE 802.11b hasta 11Mbps, y con el IEEE 802.11g hasta 54Mbps.

Tabla 3.2. Características de la Tarjeta Inalámbrica

Así como se analizó la tarjeta del equipo que utilizamos para las pruebas, se hace un análisis de que tipos de tarjetas y características que las mismas deben cumplir para los equipos que utilicen los usuarios de las oficinas en cuestión. Se toma en cuenta características generales como: el tipo, los estándares que cumplen y la velocidad a la que pueden transferir los datos, aspectos que se toma de acuerdo a las especificaciones del "Access Point" a implementarse. Para mejor entendimiento se muestra en la *tabla 3.3*, las características mínimas que las tarjetas inalámbricas deben tener para funcionar en los equipos de los usuarios, para que los equipos de cómputo puedan adaptarse e integrarse en la nueva red inalámbrica:

	Laptop	**Desktop**
Tipo	PCMCIA, USB.	PCI, USB.
Estándar	IEEE 802.11b, IEEE 802.11g.	IEEE 802.11b, IEEE 802.11g.
Velocidad	Para IEEE 802.11b hasta 11Mbps, IEEE 802.11g hasta 54Mbps.	Para IEEE 802.11b hasta 11Mbps, IEEE 802.11g hasta 54Mbps.

Tabla 3.3. Características Mínimas de las Tarjetas Inalámbricas.

En la *tabla 3.3* se indica características generales de las tarjetas inalámbricas, se menciona los tipos de tarjetas según en el equipo en que se la va a instalar, PCMCIA para equipos portátiles que no tienen integrada la tarjeta inalámbrica, PCI para equipos de escritorio y USB que se puede usar en equipos portátiles y de escritorio, estas tarjetas que se consigue fácilmente en el mercado, pero cabe decir que las tarjetas mencionadas no son las únicas, en la actualidad existen más tipos de tarjetas que han ido apareciendo de acuerdo a necesidades específicas de los usuarios de las redes inalámbricas.

3.2. ANÁLISIS TÉCNICO.

Según las características expuestas anteriormente sobre los dispositivos "Access Point" actualmente disponibles en el mercado se eligió uno de ellos tomando en cuenta varios aspectos técnicos que cumplen cada uno de ellos, mencionaremos la característica y el beneficio técnico que nos llevó a la elección. A continuación los siguientes aspectos.

- Un tema de mucha importancia en el ámbito general de las telecomunicaciones es el tema de la velocidad de transmisión. Actualmente existen muchos dispositivos "Access Point", dichos dispositivos cumplen estándares, para cumplir con los estándares deben cumplir con ciertos parámetros, por ejemplo, velocidad de transmisión, potencia de salida RF, alcance, etc. En este caso es de

mucha importancia que la velocidad de transmisión sea alta para que los usuarios tengan la facilidad de acceder a los servicios con rapidez. Hoy en día servicios como el Internet, correo electrónico, base de datos, etc, son de vital importancia y los usuarios desean acceder a ellos con facilidad y rápidamente, por lo que, el dispositivo a elegir debe cumplir con este requerimiento. La mayoría de dispositivos en la actualidad trabajan a las más altas velocidades de transmisión, los que cumplen con el estándar 802.11b transmiten hasta 11Mbps y los que trabajan con el estándar 802.11g transmiten a 54Mbps y actualmente algunos ya a 108Mbps, en los últimos días se ha escuchado hablar de un nuevo estándar que es el 802.11n que trabajará con velocidades superiores a los 54 y 108 Mbps pero aún tanto el estándar como los dispositivos se encuentran en pruebas.

- Los equipos inalámbricos en la actualidad tienen en un solo dispositivo varias funciones lo que beneficia en muchos sentidos a quienes implementan redes inalámbricas, la elección de un equipo debe basarse en las características de los servicios y seguridades que puede brindar un "Access Point", se puede decir que, para obtener una solución completa a las necesidades de los usuarios el equipo deberá cumplir con varias características, como son:
    - Debe hacer el trabajo de switch para que nos brinde un servicio de conexión rápida evitando colisiones y saturación de los puertos.
    - Debe tener una alta potencia de salida para que la señal no se debilite cuando los usuarios no estén tan cerca del "Access Point", además para que cuando existan obstáculos la señal no se debilite cuando los atraviese.
    - Deberá ser router o "ruteador" para que no se necesite de un computador que provea de direcciones dinámicas a los usuarios, sino que, directamente el mismo "Access Point" provea de dichas direcciones IP dinámicas a los usuarios.
    - Por último deberá tener uno o varios métodos de seguridad en redes para certificar que los usuarios se conecten sin temor a amenazas de usuarios ilegales que algún momento intenten incursionan en la red en cuestión.

3.3. ANÁLISIS ECONÓMICO.

Un aspecto muy importante el momento de tomar una decisión que influya en el costo que se tenga que pagar por un equipo, definitivamente el tema económico es de mucha importancia, y se lo debe manejar con cuidado.

Existen actualmente innumerables cantidades de equipos de diferentes marcas y de variados precios, es obvio que, existen marcas de prestigio que de alguna forma tienen precios muy elevados, por otra parte, hay equipos de marcas no muy conocidas que por el contrario sus costos son bastante bajos.

Para este caso se determinó que se escogerá un equipo de mediano precio, que después de un análisis costo – beneficio sea el que mejor solvente las necesidades expuestas y que a la vez no sea demasiado costoso.

3.4. SELECCIÓN DE EQUIPOS.

De acuerdo a los aspectos analizados anteriormente en los puntos 3.1, 3.2 y 3.3, se llegó a una conclusión, eligiendo así el equipo “Access Point” que mejor solventará las necesidades establecidas para este proyecto.

Según las características técnicas y económicas analizadas se determinó que el equipo que cumple con todos los requerimientos es el “Access Point” de marca Linksys, equipo que realiza 3 funciones a la vez, es “Access Point”, Switch y Router; además cumple con estándares como el 802.11b y 802.11g; y que tiene para escoger entre varios mecanismos de seguridad.

Cabe decir que, los otros equipos expuestos y analizados también cumplen con algunas de las características necesarias para solventar las necesidades expuestas, se ha elegido este por dos razones de importancia, estas son:

- La marca LinKsys es una marca o empresa fabricante filial de la marca Cisco, cabe decir que la marca Cisco es un de las de más prestigio en el campo de las redes en general, por lo que, esta es una gran ventaja sobre las otras marcas.
- Por otra parte, podemos resaltar que los equipos de marca Cisco son de alto costo, pero la línea Linksys con las certificaciones de calidad avaladas por Cisco son de bajo costo, un costo bastante atractivo a la hora de hacer una selección entre las tantas marcas existentes.

3.5. CONFIGURACIÓN DE LA RED.

Después de haber escogido el "Acces Point" de mejores características, se procede a hacer la configuración de la red Inalámbrica, se puede indicar que esta red es una ampliación a la red de la EPN, y se hace una configuración como punto de acceso a la misma. En la *figura 3.1.* se muestra como se amplia la red de la EPN usando un punto de acceso.

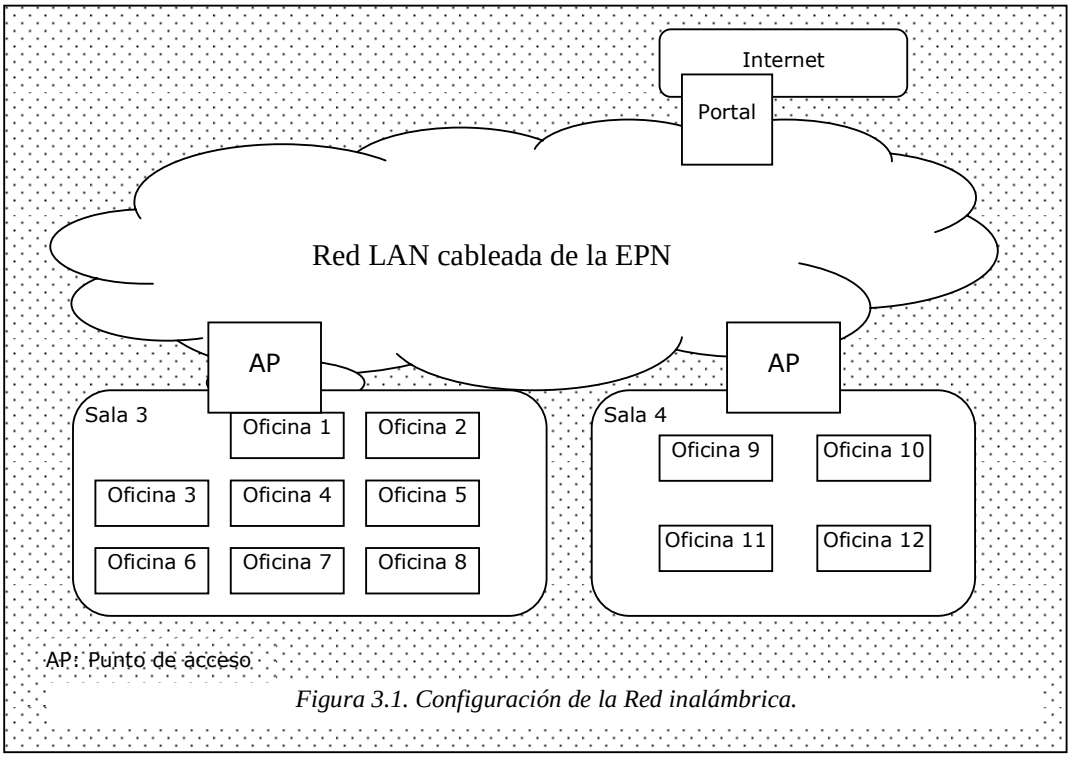


Figura 3.1. Configuración de la Red inalámbrica.

La configuración que se hace es básica, como una red inalámbrica de infraestructura, no se aplica ningún protocolo de seguridad (la configuración de seguridad la hace directamente la administración de la red de la EPN según las políticas de seguridad de esta red), únicamente se da un nombre a la red para identificarla y diferenciarla de otras redes ya existentes en el área, y se deja los parámetros de configuración por default en el equipo.

Para demostrar esta configuración se realizó los siguientes pasos:

- Luego de conectar el "Access point" en el lugar que se estima se lo va a instalar, mediante un "Patch Cord" se hace la conexión con el computador elegido para las pruebas, y siguiendo las indicaciones del manual del equipo, utilizando el Internet Explorer se conecto con la IP del equipo que por default es la

http:\\192.168.1.1, para acceder a las opciones de configuración, como se muestra en la *figura 3.2.*

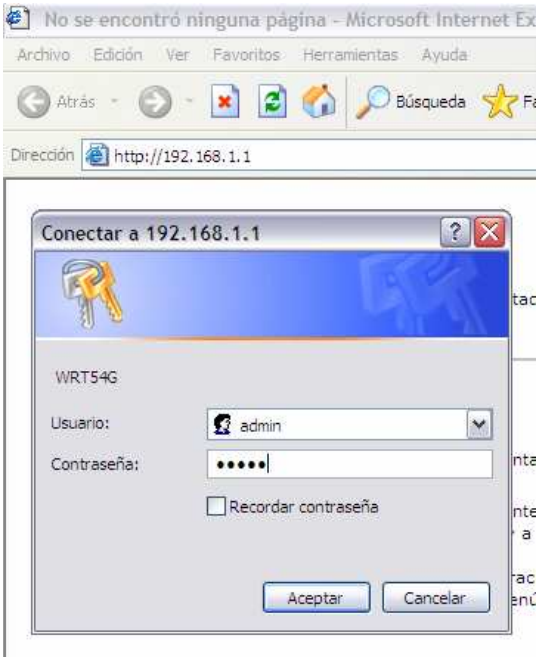


Figura 3.2. Ingreso a la Configuración del "Access Point".

- Luego se accede a la primera página de configuración del equipo, como se muestra en *figura 3.3.*

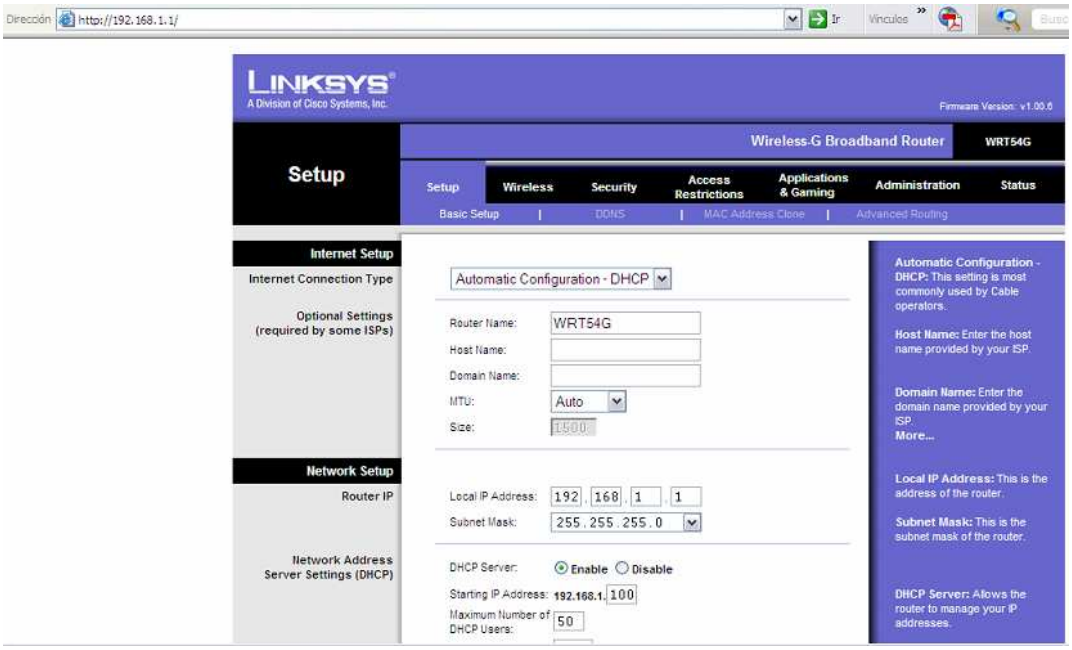


Figura 3.3. Configuración del "Access Point".

- En la opción “Wireless” de esta configuración es donde se cambia el nombre de la red, para fines de pruebas se cambió el nombre de la red por “Proyecto 34”, como se muestra en la *figura 3.4.*

Figura 3.4. Cambio de Nombre de la Red.

- Una vez hecha la configuración básica para realizar las pruebas, se procede a verificar que el “Access Point” esté enlazado a la red de la EPN, para dicha verificación se realizó pruebas haciendo ping a varias direcciones IP de equipos que están el la red como se muestra en la *figura 3.5.*

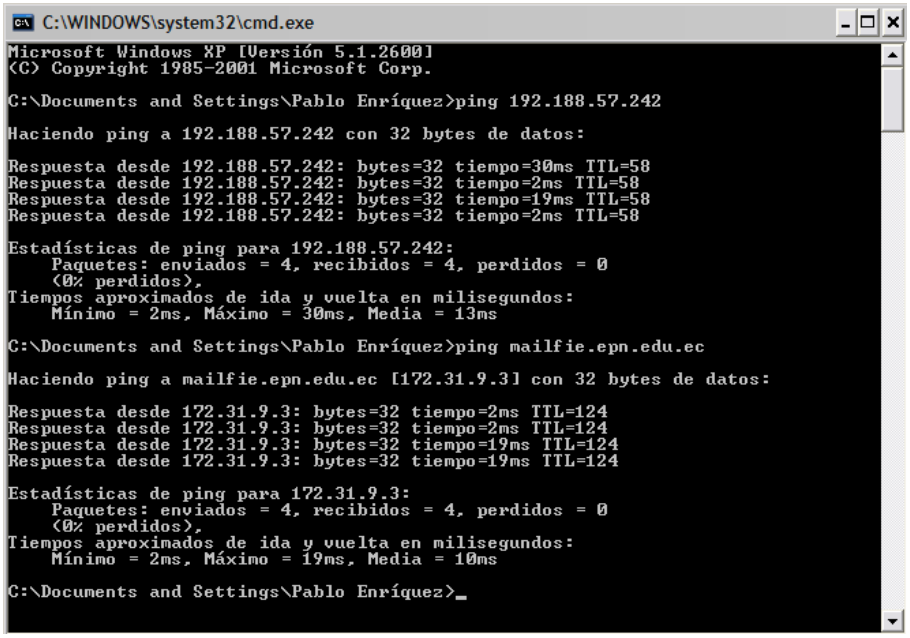


Figura 3.5. Prueba de enlace a la red de la EPN.

- Por último, para verificar que el equipo se enlazó correctamente a la red de la EPN, se verificó el estado del equipo, comprobando así, que la configuración de DHCP de la red de la EPN asignó al "Access Point" una IP automáticamente, como se puede ver en la *figura 3.6.*

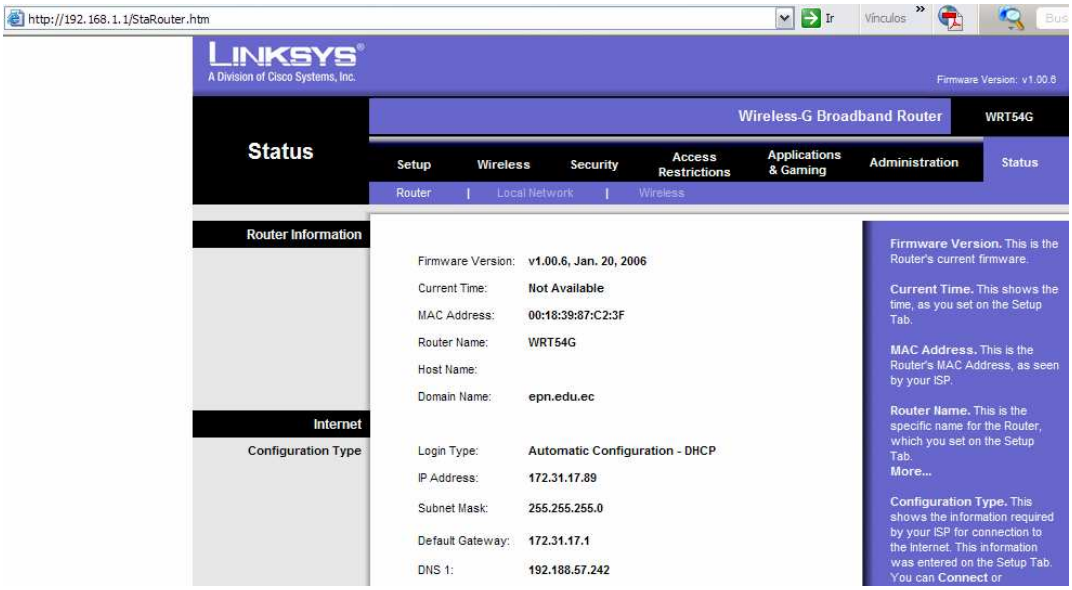


Figura 3.6. Verificación de IP en el "Access Point".

3.6. PRUEBAS DE FUNCIONAMIENTO.

Para este experimento se determinó que para asegurar el éxito del proyecto, se hagan varias pruebas de funcionamiento; básicamente pruebas con las que se pueda verificar que el equipo a usarse es el adecuado. La única prueba que garantice que el "Access Point" elegido funciona perfectamente, es una prueba hecha directamente con un equipo que recepte la señal, dicha pruebas deberá hacerse en varios lugares, en este experimento se realizó pruebas en los lugares en donde justamente van ha estar ubicados los usuarios con sus respectivos equipos de computo.

En los siguientes gráficos se ve las señales captadas y los lugares en donde fueron tomadas, además se tomó las pruebas con dos equipos "Access Point", uno de marca Linksys y otro D-Link, por lo que, en cada prueba se toma dos muestras de señal.

Para un mejor entendimiento del trabajo realizado, se explica los pasos que se siguió para tomar la pruebas. Los pasos que se siguió en la toma de pruebas de funcionamiento son los siguientes, y están ordenados según se los fue realizando:

- Se procedió a colocar el "Access Point" en un lugar estratégico de la oficina 3, tomando en cuenta a que lugares va a prestar el servicio, en la *figura 3.7.* se muestra la ubicación del "Access Point", además de los lugares donde se tomó las muestras de la potencia de la señal en cada punto. Cabe decir que en cada punto señalado se colocó el equipo laptop escogido para las pruebas, en cada uno de estos puntos se capturó una imagen que indica la potencia de la señal. Es muy importante señalar que las muestras fueron tomadas en los lugares que probablemente estarán trabajando los usuarios, pero también podemos decir que no solo ahí hay señal, como se puede ver en la *figura 3.7.* también hay señal en sectores fuera de las oficinas, como en el patio que está frente a las oficinas y en el estacionamiento que está detrás de las oficinas.

  Para este experimento hemos llamado a la red inalámbrica como "Proyecto 34" para fines de pruebas. En la *figura 3.8.* y *figura 3.9.* se ve la primera muestra de señal tomada en el mismo punto que está ubicado el "Access Point", prueba que se hizo con el fin de verificar que el "Access Point" comenzó a funcionar.

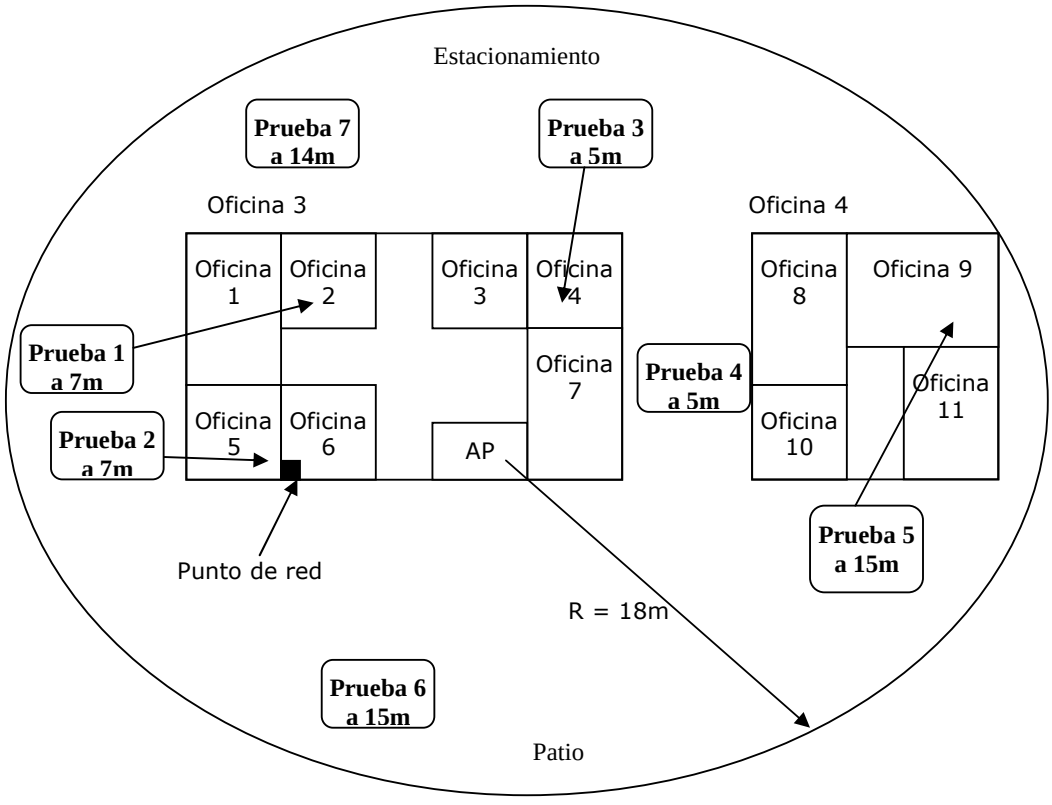


Figura 3.7. Ubicación de los Puntos de Pruebas de Funcionamiento.

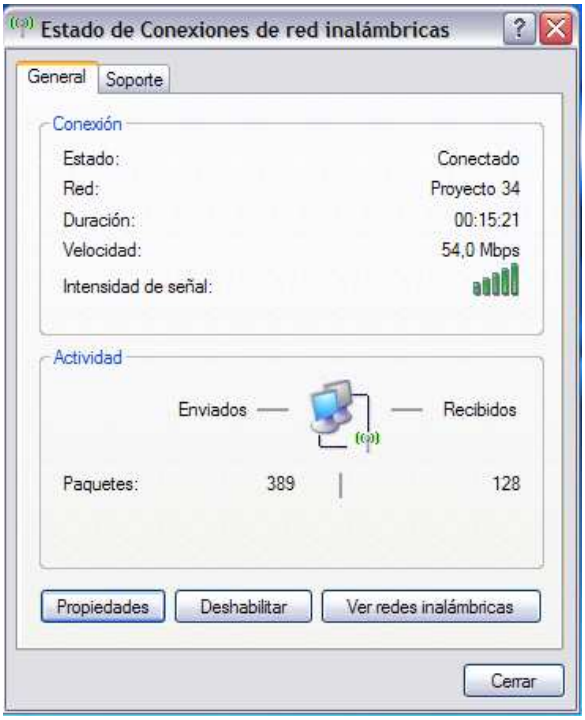


Figura 3.8. Prueba Inicial Junto al "Access Point" Linksys.

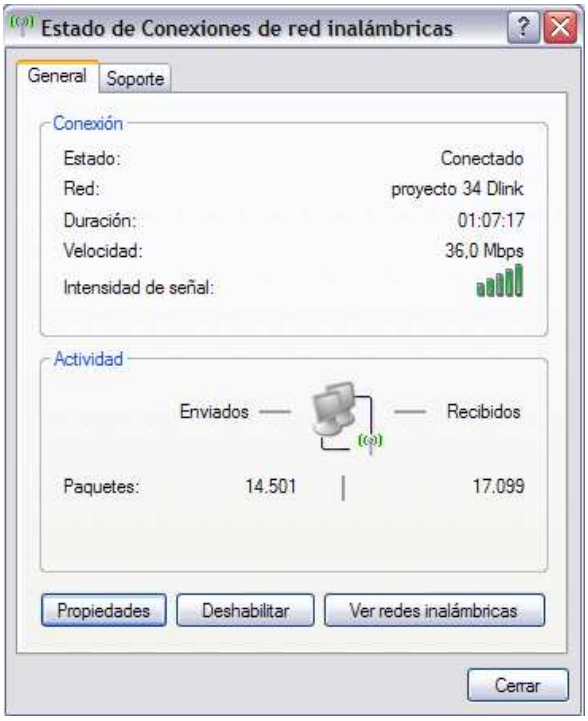


Figura 3.9. Prueba Inicial Junto al "Access Point" D-Link.

- Prueba 1. En este punto ubicado a aproximadamente unos 7 metros del "Access Point" se tomó la primera prueba, es importante decir que, este punto de prueba

está dentro de la misma sala en la que está el "Access Point" y existen como obstáculos solo estructuras o modulares separadores de oficinas, son obstáculos que no obstruyen en nada el camino de la señal y no la debilitan. En la *figura 3.10.* y *figura 3.11.* se ve la intensidad de la señal de los dos equipos.

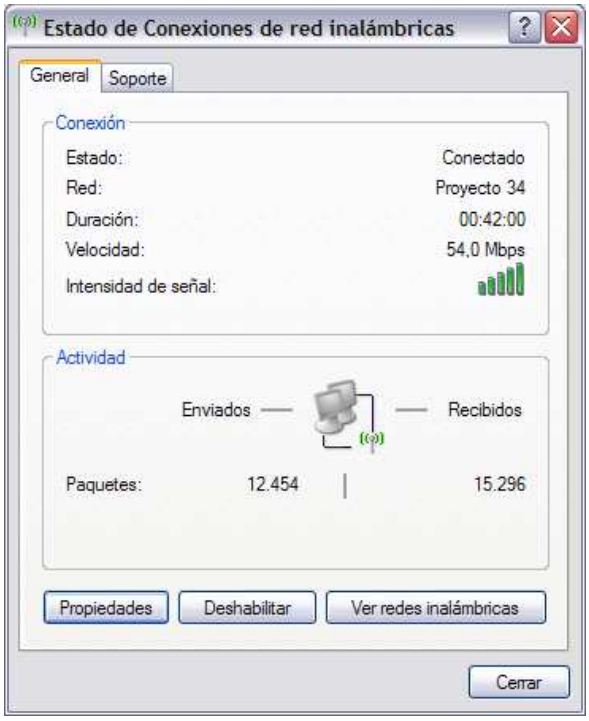


Figura 3.10. Prueba 1 Linksys.

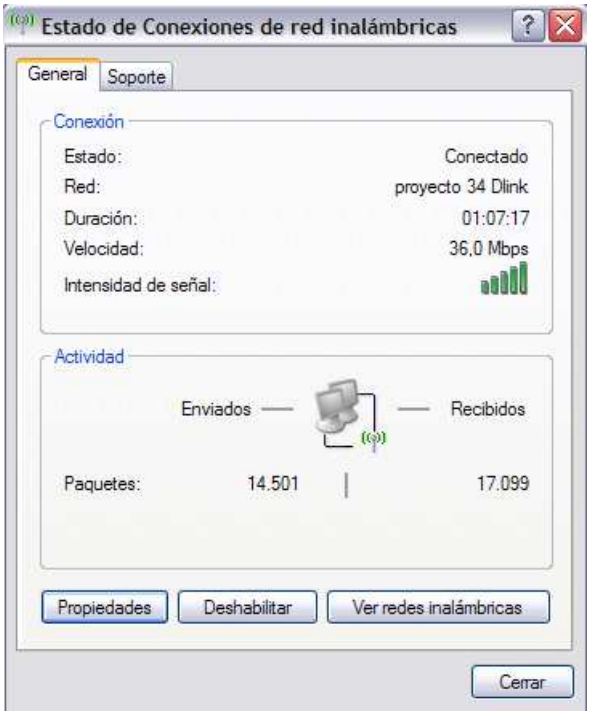


Figura 3.11. Prueba 1 D-Link.

- Prueba 2. En este punto ubicado a 7 metros del “Access Point” se tomó la segunda prueba, dentro de la misma sala 3 donde está el “Access Point” hay varios obstáculos como estructuras o modulares separadores de oficinas, en la *figura 3.12.* y *figura 3.13.* se ve la intensidad de la señal en ese punto.

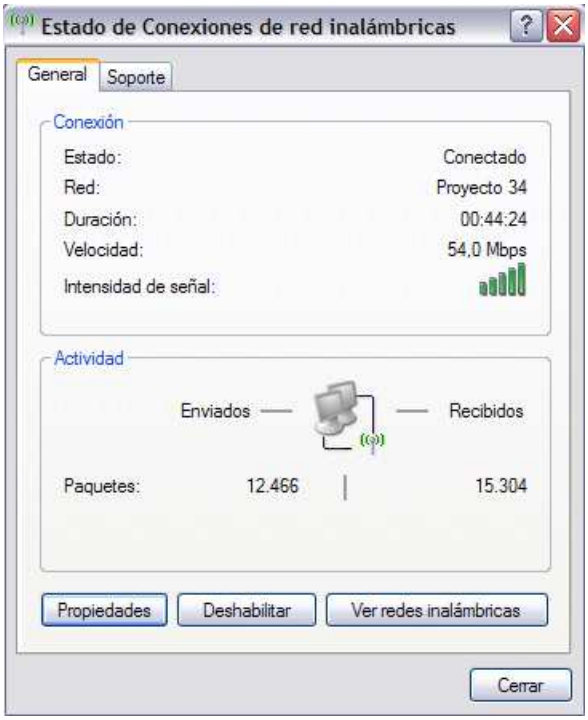


Figura 3.12. Prueba 2. Linksys.

Figura 3.13. Prueba 2. D-Link.

- Prueba 3. Esta prueba es similar a la anterior solo que en otra oficina de la misma sala, en la *figura 3.14.* y *figura 3.15.* se ve la intensidad de la señal en este punto.

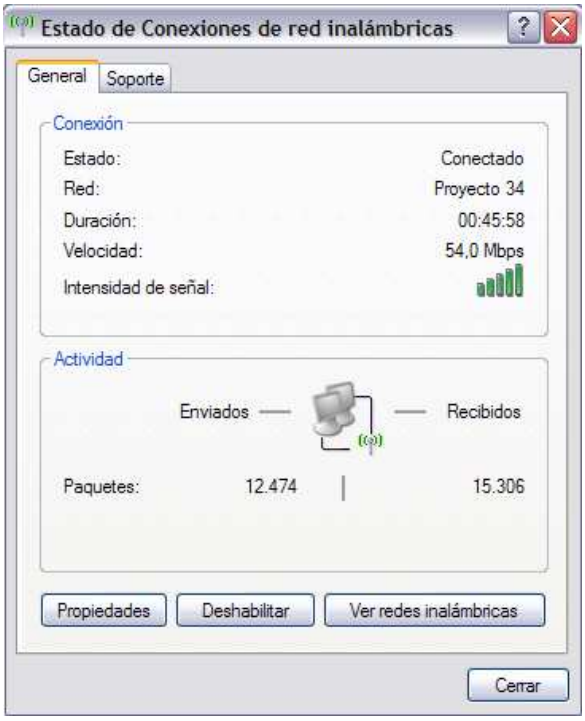


Figura 3.14. Prueba 3. Linksys.

Figura 3.15. Prueba 3. D-Link.

- Prueba 4. Esta prueba se tomó fuera de la sala 3, en el callejón que separa las salas 3 y 4, hay que indicar que para que la señal llegue a este punto tendrá que pasar por varios obstáculos, uno de ellos es una pared muy gruesa de ladrillo, en la *figura 3.16.* y *figura 3.17.* se muestra la intensidad de señal en este punto.

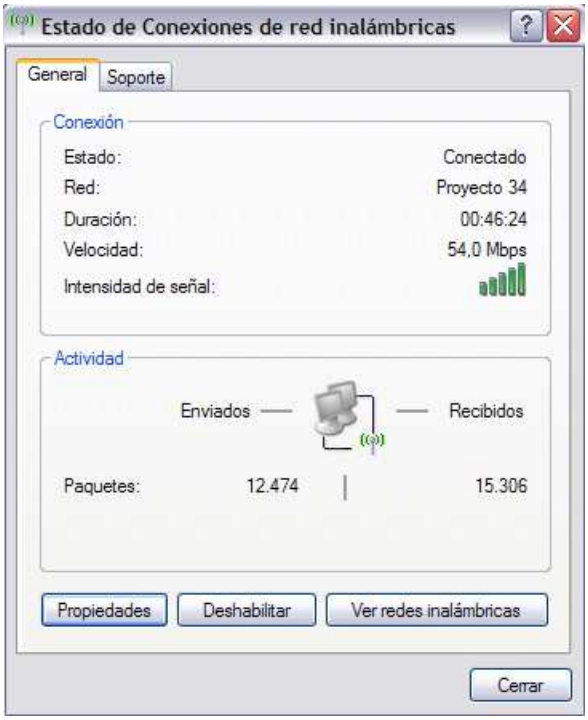


Figura 3.16. Prueba 4. Linksys.

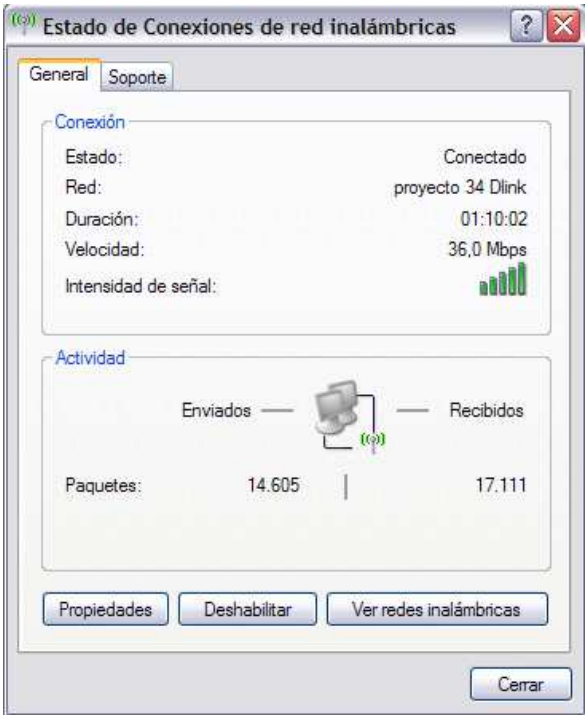


Figura 3.17. Prueba 4. D-Link.

- Prueba 5. Esta prueba se tomó fuera de la sala 3, en la sala 4, aproximadamente a 15m del “Access Point”, para que la señal llegue a este punto tendrá que pasar por más obstáculos que en los otros puntos, los más críticos son dos paredes gruesas de ladrillo que separan a las oficinas del callejón entre ellas, en la *figura 3.18.* y *figura 3.19.* se muestra la intensidad de la señal en este punto.

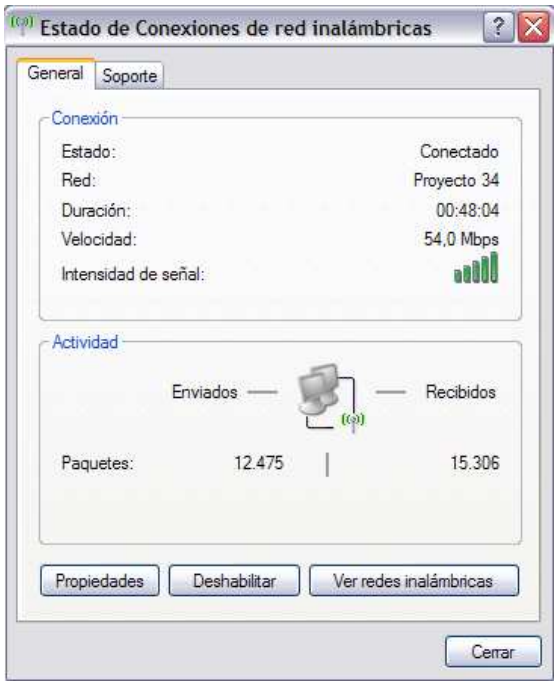


Figura 3.18. Prueba 5. Linksys.

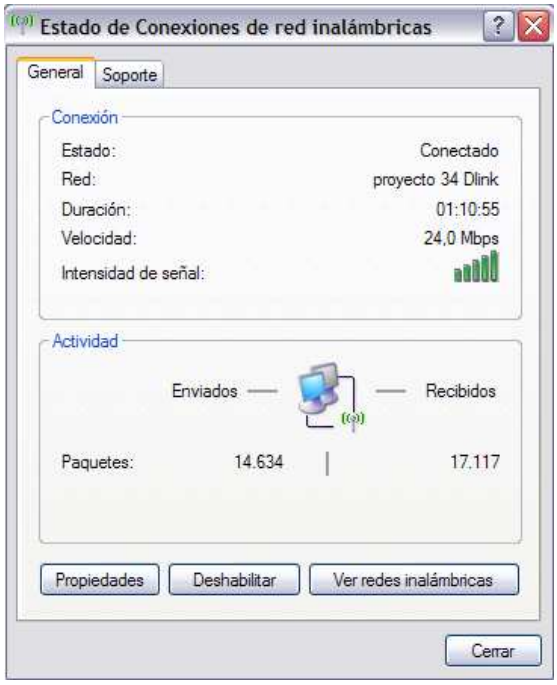


Figura 3.19. Prueba 5. D-Link.

- Prueba 6. Esta prueba se tomó fuera de la sala 3, en el patio ubicado frente a la entrada de las salas 3 y 4, la prueba se tomo a aproximadamente 15 metros del "Access Point", en la *figura 3.20.* y *figura 3.21.* se muestra la intensidad de la señal en este punto. Esta prueba se tomó con el fin de verificar el alcance del "Access Point" fuera de las salas a donde va proveer de conexión.

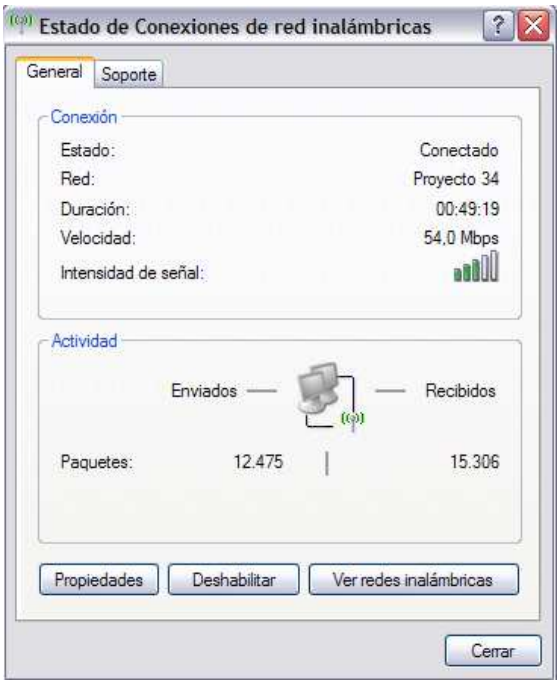


Figura 3.20. Prueba 6. Linksys.

Figura 3.21. Prueba 6. D-Link.

- Prueba 7. Esta prueba se tomó fuera de la sala 3, prácticamente en el estacionamiento ubicado detrás de las salas 3 y 4, aproximadamente a 14m del "Access Point", en la *figura 3.22.* y *figura 3.23.* se muestra la intensidad de la señal en este punto.

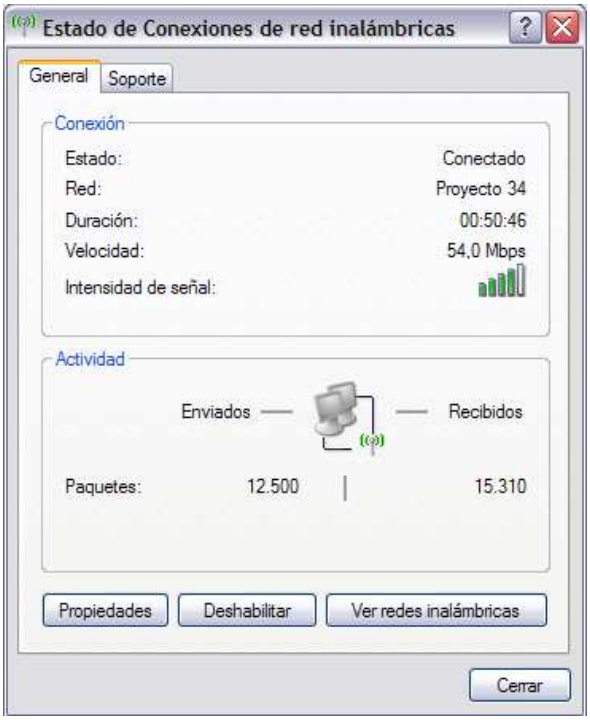


Figura 3.22. Prueba 7. Linksys.

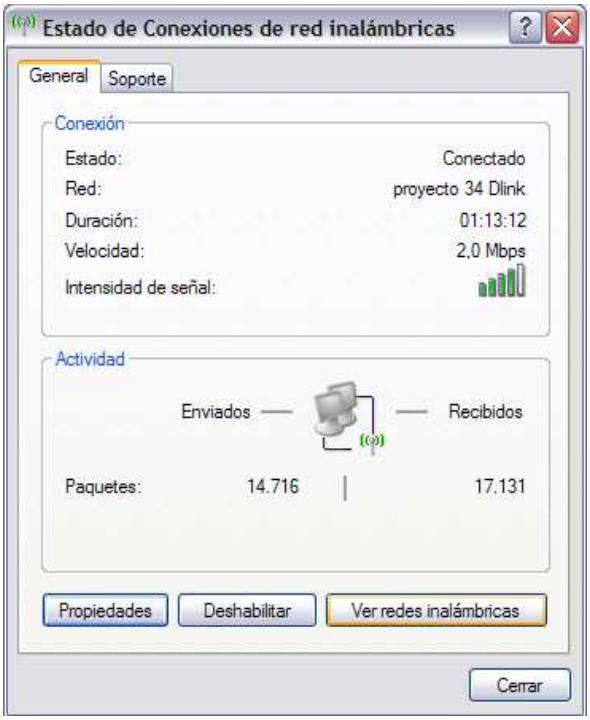


Figura 3.23. Prueba 7. D-Link.

CAPÍTULO 4.

CONCLUSIONES Y RECOMENDACIONES.

4.1. CONCLUSIONES.

- Se realizó pruebas con dos tipos de “Access Point”, uno de marca D-Link que es a la vez switch con una antena y otro de marca Linksys que es a la vez switch y router y además tiene 2 antenas, llegando a la conclusión de que según las pruebas realizadas se puede concluir que los “Access Point” Linksys que tiene dos antenas tiene mejor potencia en su señal.
- De la misma forma podemos decir que según la prueba realizada, el equipo Linksys trabaja mejor en lugares donde hay obstáculos como paredes gruesas que pueden debilitar la señal, en este experimento se pudo comprobar que este equipo tiene una buena señal aunque existen muchos obstáculos de este tipo.
- Es importante también notar que a pesar de la distancia en la que se realizó las pruebas de la señal, se obtuvo una buena respuesta del “Access Point” Linksys que no debilitaba su señal a una distancia considerable, en conclusión, este dispositivo tiene mayor alcance.
- Según la observación hecha a los dos equipos con los que se realizó pruebas, se concluyó que el que tiene dos antenas es de mejor alcance y tiene mejor señal, concluyendo así que es muy ventajoso el uso de dos antenas, ya que de alguna forma hacen un trabajo en conjunto por una parte dando una buena potencia en su señal, y por otra parte entregando la señal equitativamente a cada punto a donde la entrega.
- En la investigación realizada sobre las tarjetas inalámbricas se puede concluir que, en la actualidad la mayoría de equipos se diseñan con la opción de poder incorporar una tarjeta inalámbrica. En el caso de los equipos portátiles se puede decir que todos tienen ya incorporada la tarjeta en su hardware; en el caso de los equipos de escritorio en menoría pero algunas marcas también las incluyen, claro que en los que no están incluidas hay la opción de expansión como son las ranuras de expansión PCI y en la actualidad se utiliza bastante la opción de expansión por USB. Por lo que en este caso los usuarios que tengan equipos

portátiles no tendrán problema en conectarse inmediatamente a la nueva red, y los usuarios de equipos de escritorio tendrán facilidad en conseguir una tarjeta inalámbrica.

- Se puede concluir que la configuración del "Access Point" se la realiza para que se pueda acceder a la red de la EPN y a la vez al Internet. Actualmente la red de la EPN tiene configurado un servidor como DHCP (Dynamic Host Control Protocol) lo que facilita las cosas al momento de la configuración, según la característica del "Access Point" de ser también Router y con la configuración de DHCP, los dos se acoplan automáticamente ya que el servidor proporciona una IP dinámica al "Access Point", y éste a la vez proporciona IPs del mismo tipo a los usuarios.
- La velocidad a la que trabajará el "Access Point" para conectarse a la red de la EPN es la establecida en su configuración, que en el caso del equipo que se está utilizando se conecta según el estándar, con el IEEE 802.11b hasta 11Mbps y con IEEE 802.11g hasta 54Mbps.

4.2. RECOMENDACIONES.

- Una recomendación muy importante en cuanto a la ubicación del "Access Point" es que antes de escoger el lugar, se realice varias pruebas en varios lugares, sólo las pruebas realizadas pueden validar el correcto funcionamiento y desempeño en este caso de la red a implementarse.
- Otra recomendación acerca del servicio que prestará el "Access Point" es que según los requerimientos y necesidades que se detectó, se escoja un dispositivo que tenga incorporado en uno solo varios servicios, en este caso, escogimos el que nos solucionó varias necesidades sin tener que incurrir en altos costos de equipos, en períodos largos de implementación y configuración o en dificultades de infraestructura.
- Algo muy importante que no se puede dejar de mencionar es que, es recomendable usar equipos de marcas conocidas y mejor aún certificadas, en este caso se escogió uno de marca Linksys, que es una empresa filial de Cisco, tomando en cuenta el prestigio de la marca Cisco en el ámbito de las redes, de alguna forma esta elección nos certifica el funcionamiento de nuestro proyecto.

- La configuración del “Access Point” se la realizó siguiendo los pasos del manual de instalación del mismo, por lo que la recomendación para futuras configuraciones del mismo equipo o equipos de similares características es que se siga las instrucciones que indica el fabricante en los manuales, es muy importante seguirlas para asegurar el correcto funcionamiento del la red y los equipos, se puede decir también que siguiendo estas instrucciones se hace la configuración más rápida.
- Es muy importante saber que las tarjetas inalámbricas están diseñadas de acuerdo a los estándares que están vigentes en la actualidad, más no se puede asegurar el funcionamiento en todos los equipos, la recomendación se hace a los usuarios que usan equipos de generaciones anteriores, para que antes de elegir la tarjeta, primero se verifique en las especificaciones que da el fabricante de los requerimientos mínimos del equipo para que estas tarjetas puedan ser instaladas.

BIBLIOGRAFÍA.

Referencia	Libros
1	ANDREW S. TANENBAUM, *"Redes de Computadoras"*, cuarta edición, PEARSON EDUCATION S.A., 2003, México, Pág. 16-25; 267-270; 292-302; 780-785.
2	GARCÍA TOMÁS JESÚS; RAYA CABRERA JOSÉ LUÍS; RAYA VÍCTOR RODRIGO, *"Alta Velocidad y Calidad de Servicio en Redes IP"*, primera edición, ALFAOMEGA RA-MA, 2002, México, Pág. 47-60; 561-568.
3	PANOS C. LEKKAS; RANDALL K. NICHOLS, *"Seguridad para Redes Inalámbricas"*, primera edición, McGrawHill, 2004, Madrid, Pág. 357-377.
4	STALLINGS WILLIAM, *"Comunicaciones y Redes de Computadoras"*, séptima edición, PEARSON EDUCATION S.A., 2004, Madrid, Pág. 286-287; 558-581.
	Cursos
5	*"Curso D-Link, Empresa Akros Solutions"*, Febrero 2006, Quito - Ecuador.
6	*"Curso Redes LAN Inalámbricas"*, Ing. Fabio Gonzales, Escuela Politécnica Nacional, Abril – Agosto 2006, Quito – Ecuador.
	URLs
7	*"Configuración de Redes Inalámbricas IEEE 802_11 de Windows XP para el hogar y la pequeña empresa"* http://www.microsoft.com/spain/technet/recursos/articulos/wifisoho.mspx#E5B
8	*"Tecnologías de redes inalámbricas y Windows XP"* http://www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp
9	*"Protocolos de Seguridad en Redes Inalámbricas"* http://www.saulo.netpubinvSegWiFi-art.htm
10	*"Contribución de Intel al Estándar IEEE 802_11 para WLAN"* http://www.intel.com/cd/personal/computing/emea/spa/wireless/245838.htm#
11	*"Wireless network interface card"* http://en.wikipedia.org/wiki/Wireless_card
12	*"Wireless access point"* http://en.wikipedia.org/wiki/Access_point
13	*"Redes Locales Inalámbricas"* http://www.unincca.edu.co/boletin/indice.htm

ÍNDICE

ANEXO A.
A1. PROFORMA EQUIPO D-Link

Somos contribuyentes especiales

Quito, 24/04/2007

Señor:
PABLO ENRIQUEZ
Atte.

Ciudad.-
Presente.-

En atención a su gentil requerimiento, ponemos a su disposición nuestra oferta de lo siguiente:

DESCRIPCIÓN	CANTIDAD	PRECIO UNIDAD USD	PRECIO TOTAL USD
DI-624 ACCROUTER+ACCESS POINT+SWITCH 4PTOS WIRELESS D-LINK 802.11G 108MBPS	**1**	110,00	110,00
		Valor Neto Total	**$ 110,00**
		12% IVA	**$ 13,20**
		Valor Total Final	**$123,20**

IMPORTANTE:

Condiciones de Negociación:

- Tiempo de Entrega: inmediata , previa consulta de stock

- Forma de pago: contado

- **Validez de la Oferta: 5 días.**

República 311 (E7-320) y Almagro, Esquina. PBX: 2502334, 2907676, Fax: 2502334, 2907676
Quito – Ecuador.
ite: www.akroscorp.com

Delia Vargas
Ejecutiva de Ventas/Area Técnica
COMPULAB - QUITO
delia.vargas@akroscorp.com
Fono: 2502334 Ext: 223

A2. PROFORMA EQUIPO Linksys

Somos contribuyentes especiales

Quito, 24/04/2007

Señor:
PABLO ENRIQUEZ
Atte.

Ciudad.-
Presente.-

En atención a su gentil requerimiento, ponemos a su disposición nuestra oferta de lo siguiente:

DESCRIPCIÓN	CANTIDAD	PRECIO UNIDAD USD	PRECIO TOTAL USD
WRT54G ACCROUTER LINKSYS-CISCO BROADBAND	**1**	85,00	85,00
		Valor Neto Total	**$ 85,00**
		12% IVA	**$ 10,20**
		Valor Total Final	**$95,20**

IMPORTANTE:

Condiciones de Negociación:
- Tiempo de Entrega: inmediata , previa consulta de stock
- Forma de pago: contado

- **Validez de la Oferta: 5 días.**

República 311 (E7-320) y Almagro, Esquina. PBX: 2502334, 2907676, Fax: 2502334, 2907676
Quito – Ecuador.
Web Site: www.akroscorp.com

Delia Vargas
Ejecutiva de Ventas/Area Técnica
COMPULAB - QUITO
delia.vargas@akroscorp.com
Fono: 2502334 Ext: 223

A3. PROFORMA EQUIPO C-Net

Somos contribuyentes especiales

Quito, 24/04/2007

Señor:
PABLO ENRIQUEZ
Atte.

Ciudad.-
Presente.-

En atención a su gentil requerimiento, ponemos a su disposición nuestra oferta de lo siguiente:

DESCRIPCIÓN	CANTIDAD	PRECIO UNIDAD USD	PRECIO TOTAL USD
CWA-854 Access Point Wireless-G Access Point C-Net	**1**	105,00	105,00
		Valor Neto Total	**$ 105,00**
		12% IVA	**$ 12,60**
		Valor Total Final	**$117,60**

IMPORTANTE:

Condiciones de Negociación:
- Tiempo de Entrega: inmediata , previa consulta de stock
- Forma de pago: contado

- **Validez de la Oferta: 5 días.**

República 311 (E7-320) y Almagro, Esquina. PBX: 2502334, 2907676, Fax: 2502334, 2907676
Quito – Ecuador.
ite: www.akroscorp.com

Delia Vargas
Ejecutiva de Ventas/Area Técnica
COMPULAB - QUITO
delia.vargas@akroscorp.com
Fono: 2502334 Ext: 223

ANEXO B.

B1. CARACTERÍSTICAS EQUIPO D-Link

D-Link

DI-624

Wireless G 108Mbps Router

AirPlusXtremeG

802.11g/2.4GHz Wireless 108Mbps[1] Router

Protect & Share Your Internet Connection

G

108Mbps

Features

- Up to 108Mbps[1] and Fully Compatible with 11g & 11b
- Advanced Firewall & Parental Control
- New Integrated Cable Diagnostic Utility
- Built-in 4-Port Switch
- Increased Security with 802.1X and WPA
- Supports VPN Multiple/Concurrent Sessions
- Free Firmware Upgrade for XR
- Bilingual Technical Support

Wi Fi CERTIFIED b g

D-Link, the industry pioneer in wireless networking, introduces another performance breakthrough in wireless connectivity—the D-Link AirPlus Xtreme G™ series of high-speed devices capable of transfer rates up to 15x faster than standard 802.11b with D-Link 108G. And with the new AirPlus Xtreme G DI-624 4-Port Wireless Router, D-Link once again sets a new standard for wireless broadband routers.

With the enhancement of D-Link 108G, the DI-624 can achieve wireless speeds up to 15x in a pure D-Link 108G environment through the use of new wireless techniques such as Packet Bursting, FastFrame, Compression & Encryption, and Turbo mode. This provides a bandwidth large enough to handle video/audio streaming and Video on Demand (VoD) applications.

The DI-624 features the very latest in advanced wireless silicon chip technology including enhanced security to shield and protect your wireless communication from intruders. It also includes D-Link's own robust firewall security features. The DI-624 is ideal for those creating their first wireless network, as well as for more advanced users looking for additional management settings and policy-based content filtering. Filters can be set based on MAC address, IP address, URL and/or Domain Name. A simple, yet intelligent, web-based setup wizard makes the DI-624 easy for any user to quickly and securely connect computers to share a high-speed Internet connection, files, resources, games or just to communicate. An integrated 4-port switch allows direct connection of up to four computers.

Several wireless clients can also securely connect to the network using WPA (Wi-Fi Protected Access), as well as 802.1X authentication, providing you a much higher level of security and authentication than has previously been available. Additional security features include VPN pass-through of multiple concurrent IPSec and PPTP sessions for telecommuters or for anyone who needs to transmit sensitive information more securely.

[1] Actual data throughput will vary. Network conditions and environmental factors lower actual data throughput rate.

The D-Link Difference

Brand Name - Local Support - Right Price

1-800-D-LINK-CA (1-800-354-6522) www.dlink.ca

D-Link

DI-624
Wireless G 108Mbps Router

AirPlusXtremeG™

802.11g/2.4GHz Wireless 108Mbps[1] Router

Specifications:

Standards
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

VPN Pass Through / Multi-Sessions
- PPTP • L2TP • IPSec

Advanced Firewall Features
(see table to right)

Device Management
- Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java- enabled browsers.
- DHCP Server and Client

Wireless Data Rates With Automatic Fallback
- D-Link 108G: 108Mbps [1]
- 54Mbps • 48Mbps
- 36Mbps • 24Mbps
- 18Mbps • 12Mbps
- 11Mbps • 9Mbps
- 6Mbps • 5.5Mbps
- 2Mbps • 1Mbps

Security
- 64/128-WEP
- 802.1X
- WPA EAP, WPA PSK

Media Access Control
CSMA/CA with ACK

Frequency Range
2.4GHz to 2.462GHz

Signal Range [2]
Indoors: Up to 328 ft (100 meters)
Outdoors: Up to 1312 ft (400 meters)

Modulation Technology
- Orthogonal Frequency Division Multiplexing (OFDM)
- Complementary Code Keying (CCK)

Receiver Sensitivity (for 802.11b)
- 11Mbps (OFDM, 10% PER,-82dBm)
- 5.5Mbps (OFDM, 10% PER,-86dBm)
- 2Mbps (OFDM, 10% PER,-90dBm)
- 1Mbps (OFDM, 10% PER,-90dBm)

Receiver Sensitivity (for 802.11g)
- 54Mbps (OFDM, 10% PER,-68dBm)
- 48Mbps (OFDM, 10% PER,-72dBm)
- 36Mbps (OFDM, 10% PER,-76dBm)
- 24Mbps (OFDM, 10% PER,-79dBm)
- 18Mbps (OFDM, 10% PER,-82dBm)
- 12Mbps (CCK, 8% PER,-86dBm)
- 9Mbps (OFDM, 10% PER,-89dBm)
- 6Mbps (OFDM, 10% PER,-90dBm)

Transmitter Output Power (for 802.11b)
1Mbps, 2Mbps, 5.5Mbps, 11Mbps:
18dBm

Transmitter Output Power (for 802.11g)
6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps:
18dBm
48Mbps, 54Mbps:
17dBm

External Antenna Type
Single detachable reverse SMA

LEDs
- Power • WAN • LAN (10/100)
- WLAN (Wireless Connection)

Operating Temperature
32°F to 131°F (0°C to 55°C)

Humidity
95% maximum (non-condensing)

Power Input
Ext. Power Supply DC 5V, 2.4A

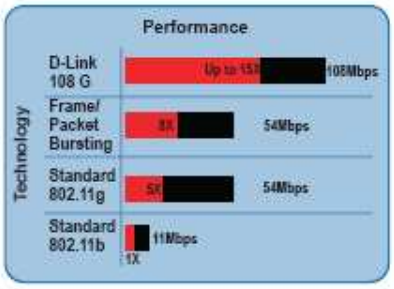
Dimensions
- L = 7.5 inches (190.5mm)
- W = 4.6 inches (116.84mm)
- H = 1.375inches (35mm)

Weight
0.66lb (298g)

Certifications
- FCC

Warranty
3 Years

[1] Environmental factors may adversely affect wireless signal range.



Advanced Firewall Features

Feature	Available
NAT with VPN Passthrough (Network Address Translation)	✓
MAC Filtering	✓
IP Filtering	✓
URL Filtering	✓
Domain Blocking	✓
Scheduling	✓

The D-Link Difference
Brand Name - Local Support - Right Price
1-800-D-LINK-CA (1-800-354-6522) www.dlink.ca

B2. CARACTERÍSTICAS EQUIPO Linksys

LINKSYS®
A Division of Cisco Systems, Inc.

The All-In-One Wireless-G Networking Solution

Secure Easy Setup

The Linksys Wireless-G Broadband Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect both screaming fast Wireless-G (802.11g at 54Mbps) and Wireless-B (802.11b at 11Mbps) devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. Connect four PCs directly, or attach more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

Once your computers are connected to the Router and the Internet, they can communicate with each other too, sharing resources and files. All your computers can print on a shared printer connected anywhere in the house. And your computers can share all kinds of files -- music, digital pictures, and documents. Keep all your digital music on one computer, and listen to it anywhere in the house. Organize all of your family's digital pictures in one place, to simplify finding the ones you want, and easing backup to CD-R. Utilize extra free space on one computer when another's hard drive starts to fill up.

The new push button setup feature makes it easy to configure your wireless devices. Just push the button on the router and on your other SecureEasySetup-enabled wireless device to automatically create an encryption-secured wireless connection. Wi-Fi Protected Access™ 2 (WPA2) protects your data and privacy with up to 128-bit industrial-strength encryption. The Router can serve as a DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. Advanced configuration is a snap with the web browser-based interface.

With the Linksys Wireless-G Broadband Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with flexibility, speed,

All-in-one Internet-sharing Router, 4-port Switch, and Wireless-G (802.11g) Access Point	Shares a single Internet connection and other resources with Ethernet wired and Wireless-G and -B devices	Push button setup feature makes wireless configuration secure and simple	High security: Wi-Fi Protected Access™ 2 (WPA2), wireless MAC address filtering, powerful SPI firewall

Wireless-G
Broadband Router

Wireless

Product Data

Model No. **WRT54G**

Cisco Systems

Wireless-G
Broadband Router

Features

- Complies with 802.11g and 802.11b (2.4GHz) Standards
- Unsurpassed Wireless Security with Wi-Fi Protected Access™ 2 (WPA2)
- Enhanced Internet Security Management Functions including Internet Access Policies with Time Schedules
- All LAN Ports Support Auto-Crossover (MDI/MDI-X) - No Need for Crossover Cables
- SecureEasySetup push button makes it easy to configure your wireless devices

Specifications

Model Number	WRT54G
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe and Japan)
Ports/Buttons	Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port One Reset Button One SES Button
Cabling Type	UTP CAT 5
LEDs	Power, DMZ, WLAN, LAN (1, 2, 3, 4), Internet
RF Power Output	18 dBm
UPnP able/cert	able
Security features	Stateful Packet Inspection (SPI) Firewall, Internet Policy
Wireless Security	Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering

Environmental

Dimensions W x H x D	7.32" x 1.89" x 7.87" (186 mm x 48 mm x 200 mm)
Weight	1.06 lbs. (0.482 kg)
Power	External, 12V DC, 0.5A
Certifications	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM
Operating Temp.	32°F to 104F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10~85% Non-condensing
Storage Humidity	5~90% Non-condensing
Warranty	3-Years

Linksys
A Division of Cisco Systems, Inc.
19592 Teller Avenue
Irvine, CA 92612 USA

E-mail: sales@linksys.com
support@linksys.com

Web: http://www.linksys.com

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- 200 MHz or faster processor
- 64 MB of RAM
- Internet Explorer 5.5 or Firefox 1.0 or Higher for Web-based configuration
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP
- Network Adapter

Package Contents

- Wireless-G Broadband Router
- Setup CD-ROM with Symantec Internet Security
- User Guide on CD-ROM
- Power Adapter
- Ethernet Network Cable
- Registration Card

WRT54G-DS-50828 KL

Product Data

Model No. WRT54G

B3. CARACTERÍSTICAS EQUIPO C-Net

TOTAL NETWORK SOLUTIONS

ORDERING INFORMATION

Model	Description
CWA-854	Wireless-G Access Point

Wireless-G Access Point

This CNet Wireless-G Access Point is an affordable IEEE 802.11b/g wireless LAN device, which is a feature-rich and high-performance solution for connecting multiple LANs in a MAN (Metro Area Network). Building an Enterprise area and MAN wireless infrastructure with the CNet Wireless-G Access Point. Users are able to access network resources including email and Internet at speed of up to 54 Mbps raw data rate. Once Users are connected, they can keep in touch with their e-mail, access the Internet, and use instant messaging to chat with friends, and share files and other resources such as printers and network storage with other computers on the network.

With CWA-854, wireless LAN users can connect at speeds up to 54 Mbps and interoperate with existing popular Wireless-B equipment. To protect your data and privacy, the CWA-854 can encrypt all transmissions with advanced security and firewall of a full-scale at a fraction of the price.

CNet also provides a family of wired and wireless LAN products that deliver the same level of security, scalability, and manageability for WLANs that customers have come to expect in their wired LAN, including Routers, Switches, Broadband Modems, and Network Adapters.

KEY FEATURES

- 64/128 bit WEP encryptions provides maximum wireless security
- Supports Wi-Fi alliance WPA and WPA2 for wireless security
- Access control screens device MAC addresses to ensure only trusted client's access the WLAN
- One 10/100 port with Auto MDI/MDI-X provide wired LAN connectivity; up to 253 (45 wireless) users.
- Wireless access control by MAC address (deny or accept)
- Supports WDS function to extend your wireless scope.

PRODUCT SPECIFICATIONS

Product Name	Wireless-G Access Point
Model Name	CWA-854
Standards	• IEEE 802.3 • IEEE 802.3u • IEEE 802.3X • IEEE 802.11b • IEEE 802.11g
Networking Protocols	TCP/IP, NetBIOS, IPX/SPX
Channels	• 1-11 (U.S.) • 1-13 (Elsewhere Worldwide) • 1-13,14 (Japan)
LAN interface	One 10/100 BaseT with RJ-45 connector
Media Support	CAT 5 Ethernet Cabling or Better
Data Rate	• IEEE 802.11b: 1, 2, 5.5, 11 Mbps • IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 10/100 Mbps (Ethernet)

Modulation	• 802.11b: CCK, DQPSK, DBPSK • 802.11g: OFDM
Dimensions (L x W x H)	• 129.5 x 78.5 x 26.7 mm (5.1" x 3.1" x 1.05")
Security	Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP and AES
Transmit Power	• IEEE 802.11b: 17dBm (typical) • IEEE 802.11g: 13dBM (typical)
Antenna	• Two detachable 2 dBi Antenna • Supports: Transmit (Single) and Receive (Diversity) Antenna
Diagnostic LEDs	• Power (Green), • Link (Green), • WLAN (Green)
Power Requirement	• 5V DC, 2.5A
Environment	• Operating Temperature: 0° ~ 45°C (32° ~ 113°F) • Storage Temperature: -20° ~ 70°C (-4° ~ 158°F) • Humidity: 10% ~ 90% Non-condensing

B4. MANUAL DE CONFIGURACIÓN DEL ACCESS POINT LINKSYS

Configuring the Wireless-G Broadband Router

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then you can use the Web-based Utility to configure the Router. For advanced users, you *may* configure the Router's advanced settings through the Web-based Utility.

This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users will use these two screens of the Utility:

- Basic Setup. On the *Basic Setup* screen, enter the settings provided by your ISP.
- Management. Click the **Administration** tab and then the **Management** tab. The Router's default password is **admin**. To secure the Router, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

To access the Web-based Utility, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.

A password request page, shown in Figure 6-1 will appear. (Non-Windows XP users will see a similar screen.) Leave the *User Name* field blank. The first time you open the Web-based Utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Then click the **OK** button.

NOTE: For first-time installation, Linksys recommends using the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the Web-based Utility.

HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.

Figure 6-1: Password Screen

The Setup Tab - Basic Setup

The first screen that appears displays the Setup tab. This allows you to change the Router's general settings. Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Internet Setup

The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your ISP.

Internet Connection Type

Choose the type of Internet connection your ISP provides from the drop-down menu.

- **DHCP.** By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.
- **Static IP.** If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.

  Internet IP Address. This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

  Subnet Mask. This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

  Gateway. Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

  DNS. Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 6-2: Setup Tab - Basic Setup

Figure 6-3: DHCP Connection Type

Figure 6-4: Static IP Connection Type

Static IP address: *a fixed address assigned to a computer or device connected to a network.*

- **PPPoE.** Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable **PPPoE**.

  User Name and Password. Enter the User Name and Password provided by your ISP.

  Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to *Keep Alive*. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

Figure 6-5: PPPoE Connection Type

- **PPTP.** Point-to-Point Tunneling Protocol (**PPTP**) is a service that applies to connections in Europe only.

  Specify Internet IP Address. This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

  Subnet Mask. This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

  Gateway. Your ISP will provide you with the Gateway Address.

  User Name and Password. Enter the User Name and Password provided by your ISP.

  Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to *Keep Alive*. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

Figure 6-6: PPTP Connection Type

- **HeartBeat Signal.** HeartBeat Signal (HBS) is a service that applies to connections in Australia only. If your ISP is Telstra, then select **HeartBeat Signal**.

  User Name and Password. Enter the User Name and Password provided by your ISP.

  Heart Beat Server. This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

  Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to *Keep Alive*. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

Figure 6-7: HeartBeat Signal Connection Type

Optional Settings

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.

Router Name. In this field, you can type a name of up to 39 characters to represent the Router.

Host Name/Domain Name. These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The default setting, **Manual**, allows you to enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1492. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, select **Auto**.

Figure 6-8: Optional Settings

Network Setup

The Network Setup section changes the settings on the network connected to the Router's Ethernet ports. Wireless Setup is performed through the Wireless tab.

Router IP

This presents both the Router's IP Address and Subnet Mask as seen by your network.

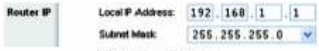


Figure 6-9: Router IP

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must configure all of your network PCs to connect to a DHCP server (the Router), and make sure there is no other DHCP server on your network.

Figure 6-10: Network Address Server Settings

DHCP Server. DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then click the **Disable** radio button (no other DHCP features will be available).

Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

Maximum Number of DHCP Users. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50.

Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

Static DNS (1-3). The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS. The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Time Setting

Change the time zone in which your network functions from this pull-down menu. (You can even automatically adjust for daylight savings time.)

Figure 6-11: Time Setting

The Setup Tab - DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com.

Figure 6-12: Setup Tab - DDNS

DDNS Service. From this pull-down menu, enter the DDNS service with which you have membership.

User Name. Enter the User Name for your DDNS account

Password. Enter the Password for your DDNS account.

Host Name. The is the DDNS URL assigned by the DDNS service.

Internet IP Address. This is the Router's current IP Address as seen on the Internet.

Status. This displays the status of the DDNS connection.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Setup Tab - MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

Figure 6-13: Setup Tab - MAC Address Clone

Enable/Disable. To have the MAC Address cloned, click the radio button beside *Enable*.

User Defined Entry. Enter the MAC Address registered with your ISP here.

Clone Your PC's MAC Address. Clicking this button will clone the MAC address.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing will automatically adjust how packets travel on your network. Static Routing sets up a fixed route to another network destination.

Figure 6-14: Setup Tab - Advanced Routing (Gateway)

Operating Mode. Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select **Gateway**. If another Router exists on your network, select **Router**. When Router is chosen, **Dynamic Routing** will be enabled.

Dynamic Routing. This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is **Disabled** by default. From the drop-down menu, you can also select **LAN & Wireless**, which performs dynamic routing over your Ethernet and wireless networks. You can also select **WAN**, which performs dynamic routing with data coming from the Internet. Finally, selecting **Both** enables dynamic routing for both networks, as well as data from the Internet.

Figure 6-15: Setup Tab - Advanced Routing (Router)

Static Routing. To set up a static route between the Router and another network, select a number from the *Static Routing* drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click the **Delete This Entry** button to delete a static route.)

Enter Route Name. Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

Destination LAN IP. The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask. The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Default Gateway. This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface. This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks), the **WAN** (Internet), or **Loopback** (a dummy network in which one PC acts like a network—necessary for certain software programs).

Click the **Show Routing Table** button to view the Static Routes you've already set up.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Wireless Tab - Basic Wireless Settings

The basic settings for wireless networking are set on this screen.

Figure 6-16: Wireless Tab - Basic Wireless Settings

Wireless Network Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed.** If you have only 802.11g devices, select **G-Only.** If you have only 802.11b devices, select **B-Only.** If you do not have any 802.11g and 802.11b devices in your network, select **Disable.**

Wireless Network Name (SSID). The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all devices in your wireless network. For added security, you should change the default SSID (**linksys**) to a unique name.

Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enable.** If you do not want to broadcast the Router's SSID, then select **Disable.**

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are four wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WEP stands for Wired Equivalent Privacy, WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is stronger than WPA. WPA Enterprise is WPA used in coordination with a RADIUS server. RADIUS stands for Remote Authentication Dial-In User Service.) These are briefly discussed here. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

IMPORTANT: If you are using WPA, always remember that each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.

WPA Personal. WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES.** Enter a WPA Shared Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

Figure 6-17: Wireless Tab - Wireless Security (WPA Personal)

WPA Enterprise. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, select the type of WPA algorithm you want to use, **TKIP** or **AES.** Enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.

Figure 6-18: Wireless Tab - Wireless Security (WPA Enterprise)

WPA2 Personal. WPA2 gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. Enter a WPA Shared Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

Figure 6-19: Wireless Tab - Wireless Security (WPA2 Personal)

WPA2 Enterprise. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, select the type of WPA algorithm you want to use, **AES**, or **TKIP + AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.

Figure 6-20: Wireless Tab - Wireless Security (WPA2 Enterprise)

RADIUS. This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Then, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Last, either generate a WEP key using the Passphrase or enter the WEP key manually.

IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

Figure 6-21: Wireless Tab - Wireless Security (RADIUS)

WEP. WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using the Passphrase or enter the WEP key manually.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

Figure 6-22: Wireless Tab - Wireless Security (WEP)

The Wireless Tab - Wireless MAC Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

Wireless MAC Filter. To filter wireless users by MAC Address, either permitting or blocking access, click **Enable.** If you do not wish to filter users by MAC Address, select **Disable.**

Prevent. Clicking this button will block wireless access by MAC Address.

Permit Only. Clicking this button will allow wireless access by MAC Address.

Edit MAC Address Filter List. Clicking this button will open the MAC Address Filter List. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click the **Wireless Client MAC List** button to display a list of network users by MAC Address.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-23: Wireless Tab - Wireless MAC Filter

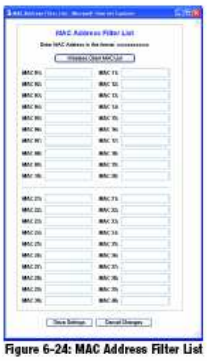


Figure 6-24: MAC Address Filter List

The Wireless Tab - Advanced Wireless Settings

This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Basic Rate. The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

Frame Burst. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Disable.**

Beacon Interval. The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM Interval. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Figure 6-25: Wireless Tab - Advanced Wireless Settings

Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

AP Isolation. This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select On. AP Isolation is Off by default.

Secure Easy Setup. This feature allows you to enable or disable the SecureEasySetup feature. Select **Disable** to disable the feature and turn off the button's light. The feature is enabled by default.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Security Tab - Firewall

Firewall Protection. This feature employs Stateful Packet Inspection (SPI) for a more detailed review of data packets entering your network environment.

Block WAN Requests. Enable the Block WAN Request feature by checking the box beside **Block Anonymous Internet Requests** and you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disabled** to allow anonymous Internet requests.

Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.

Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Select **Enabled** to filter Internet NAT redirection, or **Disabled** to disable this feature.

Filter IDENT (Port 113). This feature keeps port 113 from being scanned by devices outside of your local network. Select **Enabled** to filter port 113, or **Disabled** to disable this feature.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-26: Security Tab - Firewall

The Security Tab - VPN Passthrough

Use the settings on this tab to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.

IPSec Pass-through. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, click **Enable.** IPSec Pass-Through is enabled by default.

PPTP Pass-through. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click **Enable.** PPTP Pass-Through is enabled by default.

L2TP Pass-through. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, click **Enable.** L2TP Pass-Through is enabled by default.

Figure 6-27: Security Tab - VPN Passthrough

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Access Restrictions Tab - Internet Access

The *Internet Access* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, websites, and inbound traffic during specific days and times.

Internet Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete** button. To view all the policies, click the **Summary** button. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking the **Delete** button. To return to the Internet Access tab, click the **Close** button.)

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enable*.

You can create two kinds of policies, one kind to manage Internet access and another kind to manage inbound traffic.

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.
4. Select **Internet Access** as the Policy Type.
5. Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.
6. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
7. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

Figure 6-28: Access Restrictions Tab - Internet Access

Figure 6-29: Internet Policy Summary

Figure 6-30: List of PCs

8. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. (You can block up to 20 services.) Then enter the range of ports you want to filter.

   If the service you want to block is not listed or you want to edit a service's settings, then click the **Add/Edit Service** button. Then the *Port Services* screen will appear.

   To add a service, enter the service's name in the *Service Name* field. Select its protocol from the *Protocol* drop-down menu, and enter its range in the *Port Range* fields. Then click the **Add** button.

   To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click the **Modify** button.

   To delete a service, select it from the list on the right. Then click the **Delete** button.

   When you are finished making changes on the *Port Services* screen, click the **Apply** button to save changes. If you want to cancel your changes, click the **Cancel** button. To close the *Port Services* screen and return to the *Access Restrictions* screen, click the **Close** button.
9. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.
10. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.
11. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

Figure 6-31: Port Services

To create an Inbound Traffic policy:

1. Select **Inbound Traffic** as the Policy Type.
2. Select a number from the *Internet Access Policy* drop-down menu.
3. To enable this policy, click the radio button beside *Enable*.
4. Enter a Policy Name in the field provided.
5. Enter the source IP address whose traffic you want to manage. Select the appropriate protocol: **TCP, UDP,** or **Both.** Enter the appropriate port range, or select **Any.** Enter the destination IP address whose traffic you want to manage, or select **Any.**

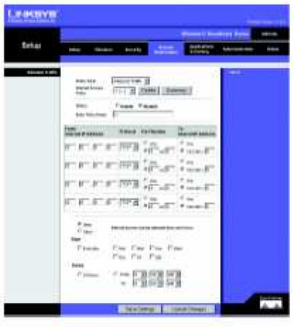


Figure 6-32: Access Restrictions Tab - Inbound Traffic

6. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow network traffic.
7. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
8. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Applications and Gaming Tab - Port Range Forward

The Applications and Gaming Tab allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

To forward a port, enter the information on each line for the criteria required. The criteria are described here.

Application. In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start/End. This is the port range. Enter the number that starts the port range under **Start** and the number that ends the range under **End.**

Protocol. Enter the protocol used for this application, either **TCP** or **UDP**, or **Both.**

IP Address. For each application, enter the IP Address of the PC running the specific application.

Enable. Click the **Enable** checkbox to enable port forwarding for the relevant application.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-33: Applications and Gaming Tab - Port Range Forward

The Applications & Gaming Tab - Port Triggering

The *Port Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Port Triggering

Application. Enter the application name of the trigger.

Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Triggered Range.

End Port. Enter the ending port number of the Triggered Range.

Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Forwarded Range.

End Port. Enter the ending port number of the Forwarded Range.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-34: Applications and Gaming Tab - Port Triggering

The Applications and Gaming Tab - DMZ

Figure 6-35: Applications and Gaming Tab - DMZ

The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forward feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

To expose one PC, select **Enable**. Then, enter the computer's IP address in the *DMZ Host IP Address* field.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Applications and Gaming Tab - QoS

Figure 6-36: Applications and Gaming Tab - QOS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

There are three types of QoS available, Device Priority, Application Priority, and Ethernet Port Priority.

Enable/Disable. To limit outgoing bandwidth for the QoS policies in use, select **Enable**. Otherwise, select **Disable**.

Upstream Bandwidth. Select the bandwidth to be used from the drop-down menu. This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use.

Device Priority

Enter the name of your network device in the *Device name* field, enter its MAC Address, then select its priority from the drop-down menu.

Ethernet Port Priority

Ethernet Port Priority QoS allows you to prioritize performance for four of the Router's ports, LAN Ports 1-4. For each of these ports, select **High** or **Low** for *Priority*. For Flow Control, if you want the Router to control the transmission of data between network devices, select **Enable**. To disable this feature, select **Disable**. The Router's other four ports will be automatically assigned low priority. Incoming Rate Limit limits the incoming

bandwidth. To use this feature, select **8M**, **4M**, **2M**, **1M**, **512K**, **256K**, or **128K** (M stands for Mbps, while K stands for kbps). If you do not want to use this feature, keep the default, **Disable**.

Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports are LAN ports going out to your network.

Application Port Priority

Application Port Priority QoS manages information as it is transmitted and received. Depending on the settings of the *QoS* screen, this feature will assign information a high or low priority for the five preset applications and three additional applications that you specify. For each application, select **High** or **Low** for *Priority*. For Specific Port#, you can add three additional applications by entering their respective port numbers in the *Specific Port#* fields.

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

HTTP (HyperText Transport Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Application Name. You can add three additional applications by entering their names in the *Application Name* fields.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Administration Tab - Management

This section of the Administration tab allows the network's administrator to manage specific Router functions for access and security.

Local Router Access. You can change the Router's password from here. Enter a new Router password and then type it again in the *Re-enter to confirm* field to confirm.

Web Access. HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web. HTTPS - Uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**. Wireless Access Web - If you are using your Wireless Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Select **Enable** to enable wireless access to the Router's web-based utility or **Disable** to disable wireless access to the utility.

Remote Router Access. To access the Router remotely, from outside the network, verify that **Enable** is selected. Then, enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual.

UPnP. When using UPnP features, select **Enable**. Because allowing this may present a risk to security, this feature is disabled by default.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-37: Administration Tab - Management

The Administration Tab - Log

The Router can keep logs of all traffic for your Internet connection. To disable the Log function, keep the default setting, **Disable**. To monitor traffic between the network and the Internet, select **Enable**. When you wish to view the logs, click **Incoming Log** or **Outgoing Log**, depending on which you wish to view.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-38: Administration Tab - Log

The Administration Tab - Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components.

Ping Test. The Ping test will check the status of a connection. Click the **Ping** button to open the *Ping Test* screen. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click the **Ping** button. The *Ping Test* screen will then display the test results. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

Traceroute Test. To test the performance of a connect, click the **Traceroute** button. Enter the address of the PC whose connection you wish to test and click the **Traceroute** button. The *Traceroute* screen will then display the test results. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 6-39: Administration Tab - Diagnostics

Figure 6-40: The Ping Test

Figure 6-41: The Traceroute Test

The Administration Tab - Factory Defaults

Click the **Yes** button to reset all configuration settings to their default values, and then click the **Save Settings** button. Any settings you have saved will be lost when the default settings are restored. This feature is disabled by default.

Figure 6-42: Administration Tab - Factory Defaults

The Administration Tab - Firmware Upgrade

Firmware can be upgraded by clicking the **Upgrade** button after browsing for the firmware, which you can download from the Linksys website. Do not upgrade your firmware unless you are experiencing problems with the Router. For more information about upgrading firmware, refer to "Appendix C: Upgrading Firmware".

Figure 6-43: Administration Tab - Firmware Upgrade

The Administration Tab - Config Management

This screen is used to back up or restore the Router's configuration file.

To back up the Router's configuration file, click the **Backup** button. Then follow the on-screen instructions.

To restore the Router's configuration file, click the **Browse** button to locate the file, and follow the on-screen instructions. After you have selected the file, click the **Restore** button.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes

Figure 6-44: Administration Tab - Config Management

The Status Tab - Router

The *Router* screen on the Status Tab displays the Router's current status.

Firmware Version. This is the Router's current firmware.

Current Time. This shows the time, as you set on the Setup Tab.

MAC Address. This is the Router's MAC Address, as seen by your ISP.

Router Name. This is the specific name for the Router, which you set on the Setup Tab.

Host Name. If required by your ISP, this would have been entered on the Setup Tab.

Domain Name. If required by your ISP, this would have been entered on the Setup Tab.

Configuration Type. This shows the information required by your ISP for connection to the Internet. This information was entered on the Setup Tab. You can **Connect** or **Disconnect** your connection here by clicking on that button.

Figure 6-45: Status Tab - Router

The Status Tab - Local Network

The *Local Network* screen on the Status Tab displays the status of your network.

MAC Address. This is the Router's MAC Address, as seen on your local, Ethernet network.

IP Address. This shows the Router's IP Address, as it appears on your local, Ethernet network.

Subnet Mask. When the Router is using a Subnet Mask, it is shown here.

DHCP Server. If you are using the Router as a DHCP server, that will be displayed here.

Start IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here.

End IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here.

DHCP Clients Table. Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a **Delete** box and clicking the **Delete** button.

Figure 6-46: Status Tab - Local Network

Figure 6-47: DHCP Clients Table

The Status Tab - Wireless

The *Wireless* screen on the Status Tab displays the status of your wireless network.

MAC Address. This is the Router's MAC Address, as seen on your local, wireless network.

Mode. As selected from the Wireless tab, this will display the wireless mode (Mixed, G-Only, or Disabled) used by the network.

SSID. As entered on the Wireless tab, this will display the wireless network name or SSID.

DHCP Server. If you are using the Router as a DHCP server, that will be displayed here.

Channel. As entered on the Wireless tab, this will display the channel on which your wireless network is broadcasting.

Encryption Function. As selected on the Security Tab, this will display what type of encryption the Router uses for security.

Figure 6-48: Status Tab - Wireless

ANEXO C.
C1. CURSO D-Link

Wireless LAN

DAC for Wireless

D-Link
1. Repasando conceptos básicos
2. Tecnología wireless
3. Productos
4. Configuración básica
5. Soluciones con wireless D-Link

1. Repasando Conceptos Básicos

IEEE 802.11

- Las velocidades de transmisión son de 1 Mbps y 2 Mbps
- Trabaja a la frecuencia de 2.4 GHz
- Permite una comunicación por tres medios:
  - Infrarojo (IR - Infrared)
  - Secuencia directa (DSSS - Direct Secuence Spread Espectrum)
  - Salto de frecuencia (FHSS – Frecuency Holding Spread Spectrum)

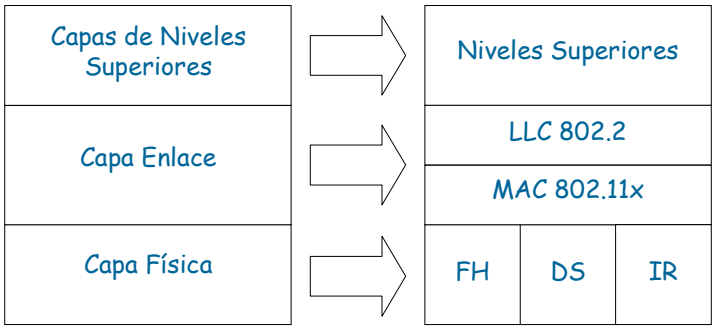
Arquitectura IEEE 802.11

- El Conjunto de Servicios Básicos (BSS – Basic Service Set) es el bloque más elemental
- Los BSS se pueden conectar a través del Sistema de Distribución (DS – Distribution System), esto permite la movilidad de los dispositivos
- Un punto de acceso es una estación que proporciona acceso a los BSS hasta el DS
- Todo el conjunto se denomina un Conjunto de Servicios Extendido (ESS – Extended Basic Set)
- Se denomina SSID al Identificador de los Servicios del Sistema de Distribución

Modelo OSI y protocolos

- Todos los estándares inalámbricos se basan el modelo de OSI (Open System Interconnection) realizado por la ISO (International Standards Organization)
- Los estándares están dentro de las dos capas más bajas del modelo OSI y son compatibles con 802.2

Modelo OSI y protocolos (cont)



Modelo de referencia OSI **Pila de protocolos**

LLC: Control Lógico del Enlace (Logical Link Control)
MAC: Control de Acceso al Medio (Medium Access Control)
FHSS: Espectro Ensanchado por Saltos de Frecuencia (Frequency Hopping Spread Spectrum)
DSSS: Espectro Ensanchado por Secuencia Directa (Direct Sequence Spread Spectrum)
IR: Infrarrojo (InfraRed)

1.1 ¿Qué es una red inalámbrica?

Red que usa el aire como medio de comunicación.
Utiliza tecnología de radio frecuencia, por ejemplo:

IEEE 802.11,
Bluetooth
Home RF y
Soluciones de Radio Frecuencia, RF

Sistema de comunicación de datos flexible Alternativo a la LAN cableada o como una extensión de ésta.

Permite mayor movilidad a los usuarios
WLAN = Wireless Local Area Network.

1.2 ¿Cómo funciona una red wireless?

Básicamente en forma similar a una red Ethernet pero teniendo como medio de transporte el aire.

En este caso el protocolo utilizado se conoce como CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

En nuestro caso para el estándar **IEEE 802.11**

1.3 Modos de operación

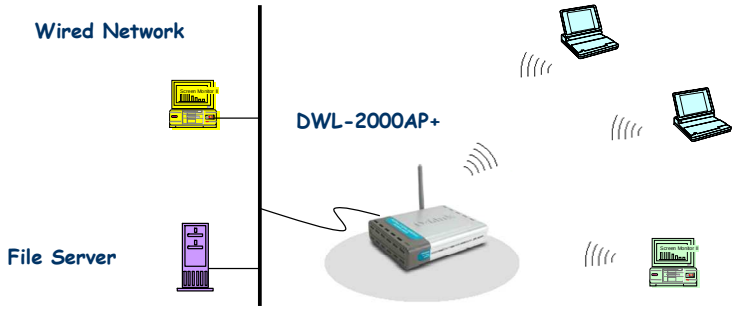
- Las formas o modos de operación o configuración son :

Ad Hoc Network. La comunicación entre las estaciones es punto a punto.

Modos de operación

Infrastructure Network.(AP)

La comunicación entre las estaciones es a través de un Access Point, el cual a su vez se conecta al cableado estructurado de la red.

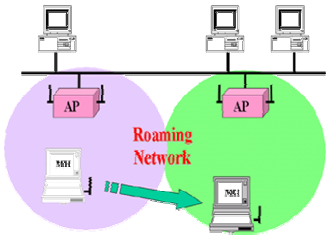


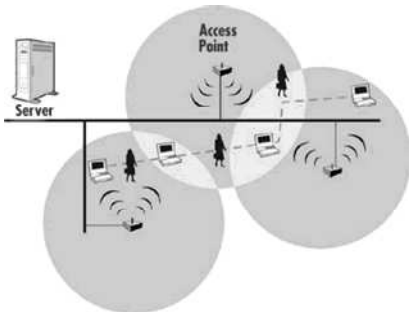
Modos de operación

Roaming.

Modo de operación que permite a una estación

Cliente "transitar a través de múltiples Access Points manteniendo la conectividad a la red.





Modos de operación

- **Infraestructura y Roaming** En este modo de operación, los APs cada 100ms envían una señal que los clientes wireless evalúan para determinar la calidad de la conexión.

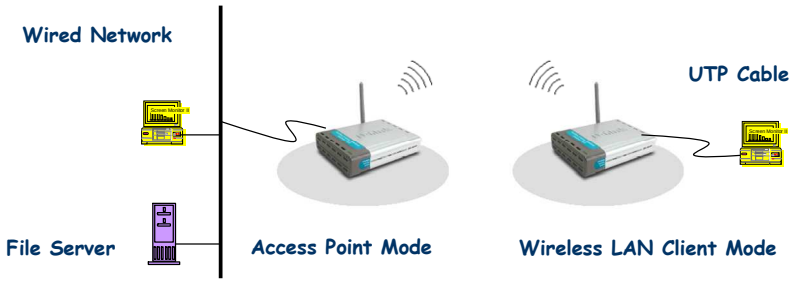
- Basados en la calidad del enlace, los clientes deciden a qué AP asociarse.

- El nuevo AP al cuál se asoció el cliente, informará de esta situación al antiguo AP, a objeto de garantizar en forma correcta la conexión del cliente.

Modos de operación

Wireless Client.

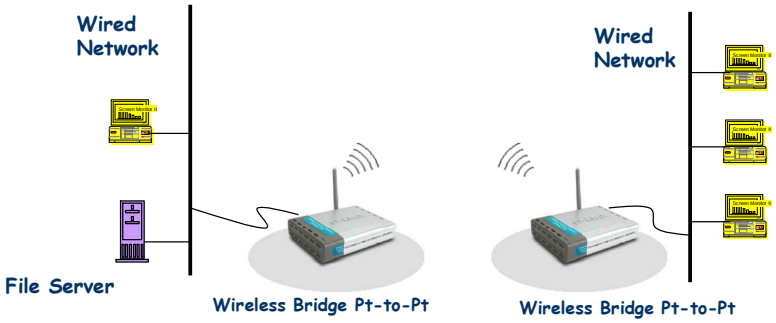
Esta modalidad transformará cualquier dispositivo Ethernet IEEE 802.3 en un cliente wireless tan pronto te conectes a un AP actuando como un Access Point.



Modos de operación

Wireless Bridge (Point to Point).

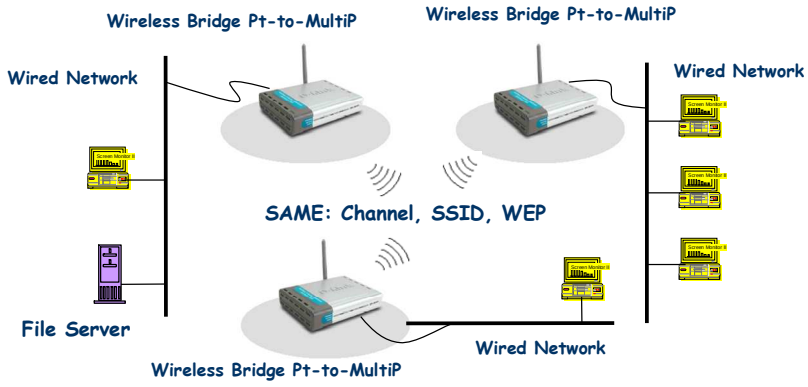
Este modo permitirá conectar dos LANs. Esta modalidad sólo trabajará con otro dispositivo Bridge.



Modos de operación

Multi-Point Bridge (Point to MultiPoint)

Este modo permitirá conectar múltiples LANs wireless.



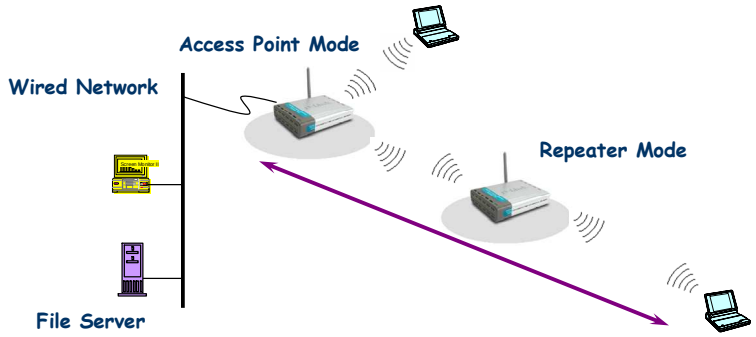
Modos de operación

Repeater

Este modo permitirá extender el rango de la red wireless.

La función Repeater trabajará con los siguientes productos:

DWL-2000AP+, DWL-2100AP, DI-624+.



1.4 Cuáles son las Principales Ventajas

- ✓Movilidad
- ✓Facilidad de instalación
- ✓Flexibilidad
- ✓Reducción de costes
- ✓Escalabilidad

1.5 Cuáles son las Aplicaciones más Utilizadas

- ✓Empresas de Manufactura
- ✓Warehouse
- ✓Servicios de Hospitales
- ✓Museos
- ✓Monumentos Nacionales
- ✓Retail

1. Tecnología Wireless

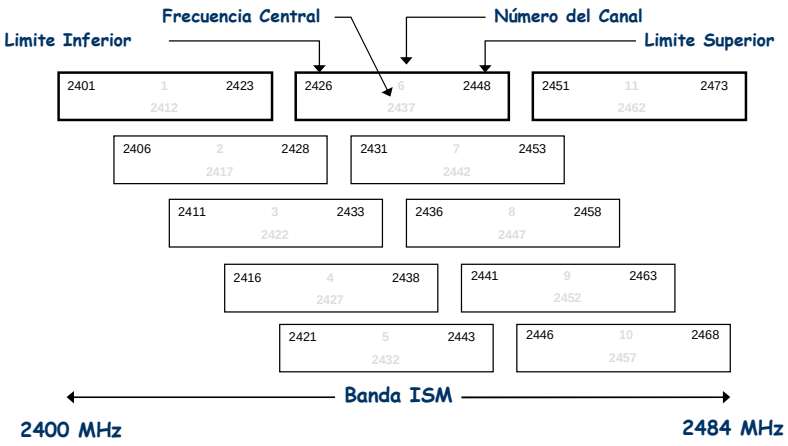
2.1 Nombre Wireless Network SSID

Nombre de la red Wireless

Cada Access Point debe ser configurado con un identificador (case sensitive ID).

Acceso seguro que sólo permite a los clientes con el correcto ID accesar la red.

2.2 Distribución de Canales



2.3 Frecuencias y Canales

- U.S.A. : 2.412 a 2.462 GHz, 11 canales
- Europa : 2.412 a 2.472 GHz, 13 canales
- Francia : 2.457 a 2.472 GHz, 4 canales
- Japón : 2.412 a 2.484 GHz, 14 canales

El Ancho de Banda de cada canal es de 20MHz.

2.4 Tasas de Transmisión

- 802.11b soporta tasas de transmisión de datos de 1, 2, 5.5 y 11 Mbps
- Mayores tasas de transferencia, mejor throughput de datos.
- Menores tasas de transferencia ofrecen más confiabilidad y mayores distancias de cobertura.
- Tasas de transferencia Auto y Fijas.

Tasas de Transmisión

- 802.11a soporta tasas de transmisión de datos de 6, 9, 12, 18, 24, 36 y 54 Mbps.
- Mayores tasas de transferencia, mejor throughput de datos.
- Menores tasas de transferencia ofrecen más confiabilidad y mayores distancias de cobertura.
- Tasas de transferencia Auto y Fijas.

Tasas de Transmisión

- 802.11g soporta tasas de transmisión de datos de 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1 Mbps,
- Mayores tasas de transferencia, mejor throughput de datos.
- Menores tasas de transferencia ofrecen más confiabilidad y mayores distancias de cobertura.
- Tasas de transferencia Auto y Fijas.

2.5 Throughput

El concepto de rendimiento se entiende de manera simplificada, como el ancho de banda efectivo -en promedio- que puede tener una red inalámbrica o alambrada. El cual en general es de un 40% del ancho de banda de la red, esto como máximo.

Por ejemplo, el rendimiento para Wireless es:

Estándar	Ancho de Banda	Rendimiento Equivalente
11b	11Mbps	4Mbps
11g	54Mbps	20Mbps
11a	54Mbps	20Mbps

Throughput

En Wireless dando como referencia o base 1 a un rendimiento menor, es decir :

Wireless 11b = 1 x

Wireless 11g, tiene un rendimiento 5 x (cinco veces) superior al rendimiento de una red Wireless 11b.

Throughput

Tipo de Red	Familia D-Link	Ancho de Banda	Abreviatura D-Link	Rendimiento Equivalente
11b	D-Link Air	11Mbps	1 x	4Mbps
11b+	D-Link AirPlus	22Mbps	2 x ó 4 x *facilidad según producto*	8Mbps ó 16Mbps
11g	D-Link AirPlus G	54Mbps	5 x	20Mbps
11g+	D-Link AirPlus G+	54Mbps	8 x	32Mbps
11g (SuperG)	D-Link Xtreme G y D-Link AirPremier AG	108Mbps	15 x	60Mbps
11a		54Mbps	5 x	20Mbps

Throughput

Los productos 1 x de D-Link tienen un rendimiento básico dentro de toda la línea de productos wireless, y que atienden principalmente las necesidades de usuarios de hogar o pequeñas oficinas.
Es decir; el rendimiento 1 x es menor que los productos 2x/4x, 5x, 8x y 15x.

Los productos 2 x / 4 x de D-Link tienen un rendimiento superior a 1x y atienden principalmente el requerimiento de usuarios de pequeñas oficinas y medianas empresas.

Los productos 5 x de D-Link tienen un rendimiento superior a 2x/4x y atienden principalmente el requerimiento de usuarios de pequeñas, medianas y grandes empresas.

Throughput

Los productos 8 x de D-Link tienen un rendimiento superior a 5x y atienden principalmente los requerimientos de usuarios de pequeñas, medianas y grandes empresas.

Los productos 15 x de D-Link tienen un rendimiento superior a 8x y atienden principalmente las necesidades de usuarios de medianas y grandes empresas, como también el de corporaciones, en que requieren un mayor rendimiento.

2.6 Conceptos Importantes.

Super G sin Turbo:
Permite incrementar el rendimiento pero solamente conectados a 54 Mbps. Usa Dynamic Packet Bursting, Fast Frames y Compresión.

Super G con Turbo Dinámico:
Permite incrementar el rendimiento y la velocidad hasta 108 Mbps. Este modo permite conexión a dispositivos no Turbo a la red. Por lo tanto deshabilitará esta función en los dispositivos que lo poseen. Usa Dynamic Packet Bursting, Fast Frames, Compresión y Turbo.

Super G con Turbo Estático:

Permite incrementar el rendimiento y la velocidad hasta 108 Mbps. Este modo no permite conexión a dispositivos no Turbo del todo. Por dispositvos que poseen Turbo se conectarán a la red. Usa Dynamic Packet Bursting, Fast Frames, Compresión y Turbo.

Conceptos Importantes.

Packet Bursting:

Es una técnica de transmisión soportada por la especificación 802.11e QoS.

La ventaja de packet bursting es que puede aumentar el throughput cuando la comunicación es con dispositivos estándares (802.11a, 802.11b y 802.11g.

Las transmisiones son separadas por un período de tiempo DIFS (Distributed Interframe Space), después de que todos los productos deben competir por el medio wireless.

El overhead de competir por el medio y el interframe space asociado a la transmisión wireless son reducidos.

Conceptos Importantes.

Fast Frames:

Fast frames, referido también como la optimización de transmisiones dinámicas.

Aumenta el throughput de datos por el incremento del número de bits enviados por frame de datos y acelera el timing del frame.

Fast frames opera cambiando los algoritmos que determinan cómo el frame de datos está estructurado.

La técnica de tramas rápidas también está basada en el estándar 802.11e QoS.

Esta técnica duplica el número de bits enviados durante cada frame.

No interfiere con frame spacing, timing o los parámetros de ventana de disputa, esta técnica escala mejor que redes exclusivamente bursting.

Conceptos Importantes.

Compresión y Encriptación Hardware:

Xtreme G y AirPremier AG utilizan el chipset Atheros™ que emplea motores de hardware especiales para comprimir y encriptar datos. Estos motores hardware operan en tiempo real para mejorar la capacidad de tratamiento al implementar algoritmos estándares y comprimir datos antes de la transmisión y después de la recepción.

Conceptos Importantes.

Multi-Channel Bonding:

Multi-Channel Bonding abarca dos canales de radio simultáneamente. Colapsa los canales disponibles desde 12 a 6 para conseguir un mayor ancho de banda en los canales disponibles. Los canales simples y dobles no se ejecutan al mismo tiempo. Esta tecnología detecta las tramas de canal simple y de canal doble y negocia soluciones basadas en el tiempo con prioridad en proceso de canal simple.

Conceptos Importantes.

Modo de Selección:

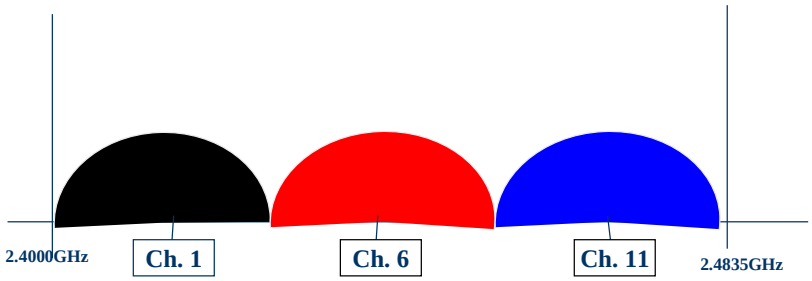
El Modo de Selección proporciona a los usuarios la opción de bloquear los productos XtremeG y AirPremier AG en un modo Estático (en vez del modo por defecto Dinámico) para alcanzar unas prestaciones todavía mayores dentro de un entorno completo D-Link de 108 Mbps.

2.7 Calidad del Enlace

- Un alto nivel de señal con un bajo nivel de ruido, provee un excelente enlace.
- Medido por la relación Señal a Nivel de Ruido (SNR)

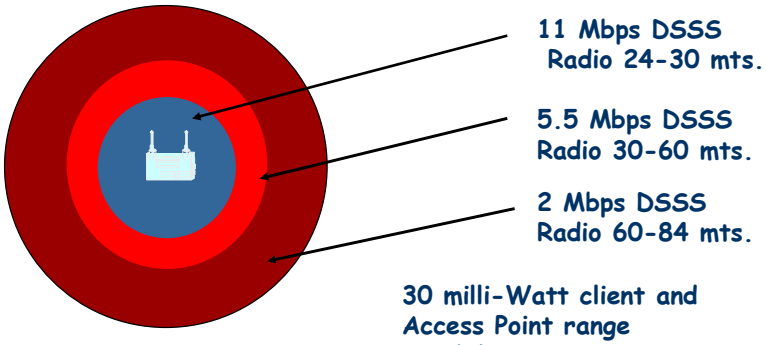
2.8 Consideraciones de Diseño

- Para maximizar el ancho de banda, los canales no deben sobreponerse.



Consideraciones de Diseño

802.11b – 30mw Cell Size Comparison



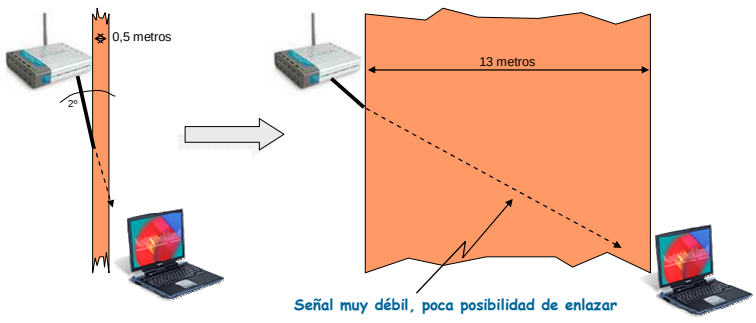
30 milli-Watt client and Access Point range capabilities

Consideraciones de Diseño

- La ubicación de los APs dependerá de las características de construcción del área.
- Murallas muy gruesas o de construcción metálica.
- Los muebles de oficina, pueden crear sombras dentro del área de cobertura.
- Interferencia de **RF** en el área de instalación de los APs.

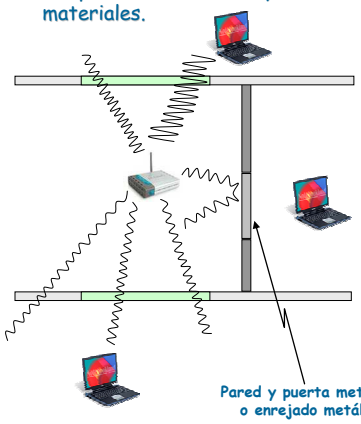
Consideraciones de Diseño

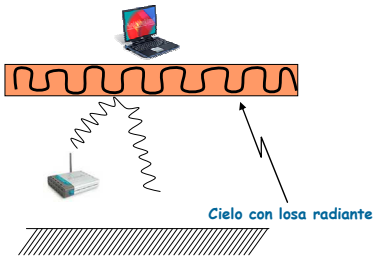
Paredes y techos - Considere lo siguiente: Una pared de 0,5 metros de espesor, en un ángulo de 45 grado, equivale casi a 1 metro. ¡En un ángulo de 2 grados esto equivale a 13 metros de espesor! Coloque sus Puntos de Acceso (AP), Gateways, y computadoras de modo que el número de paredes o techos sea minimizado.



Consideraciones de Diseño

Materiales de construcción - Una puerta sólida metálica o los postes de aluminio pueden tener un efecto negativo sobre el rango. Ponga los AP, gateways, y computadoras de modo que la señal pase por vulcanitas o entradas abiertas y no otros materiales.





Consideraciones de Diseño

- Mediante la utilización de herramientas que muestren la calidad del enlace, es posible crear un mapa de cobertura.
- Por ejemplo, el software cliente del producto Wireless.

2.9 Resumen

	802.11a	802.11b	802.11b+	802.11g
Frequency (GHz)	5.15~5.875	2.4~2.4835	2.4~2.4835	2.4~2.4835
Modulation	OFDM	DSSS with CCK	PBCC	OFDM
Speed (Mbps)	Up to 72	Up to 11	Up to 22	Up to 54
Channels	1-12 FCC 1-19 ETSI	1-11 FCC 1-13 ETSI	1-11 FCC 1-13 ETSI	1-11 FCC 1-13 ETSI
Non-Overlapping Channels	8	3	3	3
Certification	Wi-Fi	Wi-Fi	Wi-Fi	Wi-Fi
Encryption	152 bit	128 bit	256 bit	128 bit
Effective Range	Up to 30m Indoors	Up to 100m Indoors	Up to 100m Indoors	Up to 100m Indoors
Software tool (Wireless Adapters)	Linkmon	Configuration Utility	Configuration Utility	Configuration Utility

3.13 Tipo de Antenas

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas.

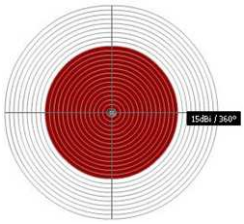
Aumentan la zona de influencia / cobertura de nuestros productos inalámbricos, de manera que en lugar de dar cobertura a unos pocos metros, podemos alcanzar cientos de metros sin problemas.

Básicamente encontramos dos tipos de antenas:

- Antenas Omnidireccionales
- Antenas Direccionales

3.14 Antenas Omnidireccionales

Cobertura con diagrama de radiación circular (360°)



Los diagramas son óvalos, debido a la cercanía con las frecuencias microondas.

Antenas Omnidireccionales

ANT24-500 5dBi

ANT24-1500 15dBi

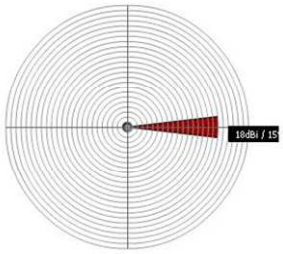
ANT24-800 8dBi

ANT24-400 4dBi

ANT24-401 4dBi
Ceiling Mount

3.15 Antenas Direccionales

- ✓ Patrón de radiación muy fuerte en dirección específica
- ✓ Focaliza radiación de la energía



Antenas Yagi, Patch y Paral

D-Link
Building Networks for People

Antenas Direccionales

ANT24-1201 12 dBi
Directional Yagi

ANT24-1801 18 dBi
Directional Yagi

ANT24-1800 18 dBi
Directional Panel

ANT24-1200 12dBi
Directional Panel

ANT24-1400 14 dBi
Directional Panel

ANT24-0801 8.5 dBi
Pico Cell Patch

ANT24-2100 21 dBi
Directional Panel

D-Link
Building Networks for People

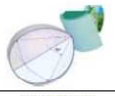
3.16 Tabla de Antenas Indoor/Outdoor

					
Model Name	DWL-R60AT	DWL-M60AT	ANT24-0400	ANT24-0401	ANT24-0500
Signal directivity	Directional Antenna	Directional Antenna	Omni-directional	Omni-directional	Omni-directional
Application range	Indoor only	Indoor only	Indoor only	Indoor ceiling only	Indoor/ Outdoor
Gain (Without cable loss)	6dBi	6dBi	4dBi	3.5dBi	5dBi
Approximate Range at 1 Mbps *	60M	60M	40M	40M	40M
Approximate Range at 11 Mbps *	25M	25M	15M	15M	15M
Half power beam width **	H60 V90	H80 V80	H360 V40	H360 V120	H360 V30
Pigtail cable length	NA	150cm	150cm	NA	30cm
Antenna fixed connector	RP-SMA plug	RP-SMA plug	RP-SMA plug	SMA jack	N-jack
Surge protector for outdoors	---	---	---	---	Optional
Default extension cable length	NA	NA	NA	2M	3M
Default mounting configuration	NA	Wall/ desktop	Wall/ desktop	Ceiling	Pole
Antenna-kit weight (Kg)	300g	330g	320g	310g	540g
Optional accessories	ANT24-JC For DWL-660 links	ANT24-JC For DWL-660 links	ANT24-JC For DWL-660 links	ANT24-JC For DWL-660 links	ANT24-JC ANT24-SP ANT24-CB series

*1.Extended range reference based on RF-Output Power 14dbm with default cable loss
*2.The transmission distance range might depend on the two same spec antennas with default cable loss
**HPBW: Half Power Beam Width. H : horizontal plane pattern, V : vertical plane pattern
The actual Indoor range will be effected by users' physical environment. The above figures are reference.

D-Link
Building Networks for People

Tabla de Antenas Indoor/Outdoor

					
Model Name	**ANT24-0800**	**ANT24-0801**	**ANT24-1200**	**ANT24-1201**	**ANT24-1400**
Signal directivity	Omni-directional	Directional	Directional	Directional	Directional
Application range	Outdoor	Outdoor	Indoor only	Outdoor	Outdoor
Gain (Without cable loss)	8dBi	8.5dBi	12dBi	12dBi	14dBi
Approximate Range at 1 Mbps *	1Km under FCC 800M under ETSI	1.2Km under FCC 800M under ETSI	2Km under FCC 1Km under ETSI	2.5Km under FCC 1Km under ETSI	3Km under FCC 1.5Km under ETSI
Approximate Range at 11 Mbps *	300M under FCC 200M under ETSI	350M under FCC 200M under ETSI	600M under FCC 300M under ETSI	750M under FCC 300M under ETSI	900M under FCC 300M under ETSI
Half power Beam width **	H360 V15	H70 V70	H80 V23	H50 V50	H30 V30
Pigtail cable length	NA	30cm	NA	30cm	30cm
Antenna fixed connector	N-jack	N-jack	SMA jack	N-jack	N-jack
Surge protector for outdoors	Included	Included	---	Included	Included
Default Extension Cable Length	50cm	3M	3M	50cm	50cm
Default mounting configuration	Pole	Wall/ pole	Window/ wall	Wall/ pole	Wall/ pole
Antenna-kit weight (kg)	1.4Kg	1.04Kg	530g	380g	2.35Kg
Optional accessories	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series

*1.Extended range reference based on RF-Output Power 14dbm with default cable loss
*2.The transmission distance range might depend on the two same spec antennas with default cable loss
**HPBW: Half Power Beam Width. H : horizontal plane pattern, V : vertical plane pattern
The actual Indoor range will be effected by users' physical environment. The above figures are reference.

D-Link
Building Networks for People

Tabla de Antenas Indoor/Outdoor

				
Model Name	**ANT24-1800**	**ANT24-1801**	**ANT24-1500**	**ANT24-2100**
Signal directivity	Directional	Directional	Omni-directional	Directional
Application range	Outdoor	Outdoor	Outdoor	Outdoor
Gain (Without cable loss)	18dBi	18dBi	15dBi	21dBi
Approximate Range at 1 Mbps *	5Km under FCC 1.2Km under ETSI	5Km under FCC 1.2Km under ETSI	5 Km	10 Km
Approximate Range at 11 Mbps *	1.5Km under FCC 300M under ETSI	1.5Km under FCC 300M under ETSI	1.5 KM	2.8 Km
Half power Beam width **	H15 V15	H15 V15	H360 V5	H18 V12
Pigtail cable length	NA	NA	NA	NA
Antenna fixed connector	N-jack	N-jack	N-jack	N-jack
Surge protector for outdoors	Included	Included	Included	Included
Default Extension Cable Length	50cm	50cm	3M	3M
Default mounting configuration	Wall/ pole	Pole	Pole	Pole
Antenna-kit weight (Kg)	3.2Kg	4.22Kg	2.5Kg	4Kg
Optional accessories	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series	Ultra low loss cable For ANT24-CB series

*1.Extended range reference based on RF-Output Power 14dbm with default cable loss
*2.The transmission distance range might depend on the two same spec antennas with default cable loss
**HPBW: Half Power Beam Width. H : horizontal plane pattern, V : vertical plane pattern
The actual Indoor range will be effected by users' physical environment. The above figures are reference.

D-Link
Building Networks for People

3.17 Relación Distancia Transmisión de Antenas

D-Link Antenna Transmission Distance (none regulated configurations)

Data Transmision speed: 11Mbps — Unit: km

Antennas		Gain (Receiver)				
		18dBi	14dBi	8dBi	6dBi	5dBi
Gain (Sender)	18dBi	5.5	4	1.5	1	0.6
	14dBi	2.5	2.5	1.5	0.8	0.6
	8dBi	1	1	1	0.8	0.6
	6dBi	0.8	0.8	0.8	0.8	0.6
	5dBi	0.8	0.6	0.6	0.6	0.5

Data Transmision speed: 5.5Mbps — Unit: km

Antennas		Gain (Receiver)				
		18dBi	14dBi	8dBi	6dBi	5dBi
Gain (Sender)	18dBi	6	4.4	1.7	1.1	0.7
	14dBi	3	3	1.7	0.9	0.7
	8dBi	1.1	1.1	1.1	0.9	0.7
	6dBi	0.9	0.9	0.9	0.9	0.7
	5dBi	0.9	0.7	0.7	0.7	0.6

Data Transmision speed: 2Mbps — Unit: km

Antennas		Gain (Receiver)				
		18dBi	14dBi	8dBi	6dBi	5dBi
Gain (Sender)	18dBi	7.15	5.2	2	1.3	0.8
	14dBi	3.5	3.5	2	1.1	0.8
	8dBi	1.3	1.3	1.3	1.1	0.8
	6dBi	1.1	1.1	1.1	1.1	0.8
	5dBi	1.1	0.8	0.8	0.8	0.7

Notas:
RF Power: 14 dBm
Low Noise Cable: ULA-168
Largo Cable: 6 Mts.
SOLAMENTE Referencia