UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

ESTUDIO DE ACCESO INALÁMBRICO A INTERNET EN CU

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

PRESENTA:

ADOLFO ANTONIO RAMÍREZ PULIDO

DIRECTOR DE TESIS: DR. JAVIER GÓMEZ CASTELLANOS

CIUDAD UNIVERSITARIA

A mi mamá,
Con todo mi corazón.

Agradecimientos

Esta tesis está dedicada a mi mamá, **Ana María Pulido Campos**, quien hizo de mí una persona de provecho para la sociedad y es mi ejemplo a seguir por sus cualidades de justicia, constancia, inteligencia y amiga. ME SIENTO MUY ORGULLOSO DE TENERLA COMO MAMÁ y es sabido que la amo con todo mi corazón.

A mi trío de hermanos, Karla Ramírez Pulido, Gabriela Paola Ramírez Pulido y Brandy Ramírez Pulido, quienes siempre me apoyaron y compartieron conmigo algunos sufrimientos y desesperanzas, pero siempre me enseñaron a seguir adelante, los quiero como nunca mugrosos (en el fondo… de mi corazón… jajaja).

A mi novia, Paola Soto Salinas, quien ha estado para animarme y enseñarme que no todo es la escuela o el trabajo; a ser más consciente de lo que pasa a mi alrededor y a "decir te quiero sin que suene a hoja en blanco", no sabes como te quiero.

Agradezco muy especialmente a la familia Del Río Pulido, quienes son personas muy cercanas a mí y que no lo hubiera podido lograr sin su ejemplo (Federico del Río Portilla), sus discusiones (Alejandra Pulido Campos), su compañía (Ana Daniela Del Río Pulido) y su picardía (Erik Federico Del Río Pulido), pero especialmente por los momentos felices que he pasado con ustedes.

A mi tía Guadalupe Pulido Campos, que es como mi segunda madre, por cuidarme todo este tiempo y por enseñarme tantas cosas que valoro muchísimo, a mis tíos, Beatriz Pulido Campos, Antonio Pulido Campos y Rosario Pulido Campos porque siempre me permitieron desarrollarme y me educaron con el ejemplo.

Agradezco a mis amigos de la carrera, quienes me brindaron su compañerismo y amistad durante tantos años; Ximena Pliego, Felipe Sánchez, Felipe Montes de Oca, Lalo, Armando Mondragón, Juan Zárraga, Javier Rodríguez, Michel, José Luís Mendoza, Toño Lima, y en especial a Salvador, Mariano y Jorge, mis hijos adoptivos.

Le agradezco a mi mejor amigo Mefi, que siempre está cuando lo necesitas y es un amigo incondicional, gran persona y corazón de pollo; ¡gracias por ser mi amigo!

A todos mis profesores que compartieron sus conocimientos conmigo y que se esforzaron y sacrificaron algo para enseñarme.

Y finalmente le agradezco a mi papá, quien me apoyo durante la carrera con valiosos consejos y a pesar de todo estuvo ahí cuando lo necesite.

Estudio de Acceso Inalámbrico a Internet en CU

Índice temático

Estudio de Acceso Inalámbrico a Internet en CU

Índice de Figuras

Estudio de acceso inalámbrico a Internet en CU

Índice de Tablas

I. Introducción

En 1887 Heinrich Rudolph Hertz, un físico alemán, demostró que existían las ondas electromagnéticas y que éstas podían ser usadas como un medio de transporte de información a muy grandes distancias. Es por esto que en nuestros días la unidad con las que son medidas las frecuencias del espectro lleven su apellido (Hertz o Hz).

La base teórica de las ondas electromagnéticas fue desarrollada mucho antes por el físico escocés James Clark Maxwell en 1864. El primer uso de las ondas electromagnéticas fue la telegrafía inalámbrica. Este relevante acontecimiento sería el predecesor de la propagación electromagnética o transmisión de radio.
Utilizando estos conceptos, el italiano Guillermo Marconi inventa la radio en 1901. La radio fue el primer medio masivo de comunicación inalámbrica y a poco más de 100 años de su invención, las comunicaciones móviles han demostrado ser una alternativa a las redes cableadas para ofrecer nuevos servicios que requieren gran ancho de banda, pero con otros beneficios como la movilidad y estar comunicado en cualquier lugar, en cualquier momento.

Algunos de los beneficios que brindan las comunicaciones inalámbricas en comparación con las redes cableadas son los siguientes:

- Capacidad para un gran número de suscriptores.
- Uso eficiente del espectro electromagnético debido a la utilización repetida de frecuencias.
- Compatibilidad a nivel nacional e internacional, para que los usuarios móviles puedan utilizar sus mismos equipos en otros países o áreas.
- Prestación de servicios para aplicaciones de datos, voz y video.
- Adaptación a la densidad de tráfico; dado que la densidad de tráfico es diferente en cada punto de la zona de cobertura.

La evolución de las redes inalámbricas está íntimamente relacionada con la evolución de los sistemas celulares y es por eso que me permito poner una breve reseña de cómo han evolucionado las redes celulares.

Las primeras redes celulares móviles

En los 1920s, en Detroit, Estados Unidos, nacen las primeras redes de comunicación móvil. Eran sistemas de radiocomunicación utilizados por el cuerpo de policía que trabajan en ese entonces a una frecuencia de 2 MHz. Una década más tarde fueron utilizados por la policía de la ciudad de Nueva York. El sistema se fue perfeccionando conforme transcurrían los años hasta que en la década de los 50 se establecieron las primeras dos bandas tal y como las conocemos ahora; la banda de VHF de radio en 150 MHz y la banda de UHF de radio en los 450 MHz. Un dato curioso es que solamente policías contaban con radio en los automóviles, ya que eran demasiado caros y ocupaban gran parte del automóvil.

En 1973 Martin Cooper introduce el primer radioteléfono mientras trabajaba para la compañía Motorota. A Cooper, pionero en esta tecnología, se le considera como "el padre de la telefonía celular". En 1979 aparece el primer sistema comercial en Tokio Japón por la compañía NTT (Nippon Telegraph & Telephone Corp.) dos años más tarde en Estados Unidos surge también el primer sistema celular analógico comercial que trabajaba en la banda de los 800 MHz. En otros países ocurrió lo mismo y surgieron muchas tecnologías paralelas pero incompatibles entre sí.

En 1981 en los países Nórdicos se introduce un sistema celular similar a AMPS (Advanced Mobile Phone System). Por otro lado, en los Estados Unidos gracias a que la entidad reguladora de ese país adopta reglas para la creación de un servicio comercial de telefonía celular, en octubre de 1983 se pone en operación el primer sistema comercial en la ciudad de Chicago. A partir de entonces en varios países se diseminó la telefonía celular como una alternativa a la telefonía convencional alámbrica. La tecnología inalámbrica tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a saturar el servicio, por lo que hubo la imperiosa necesidad de desarrollar e implementar otras formas de acceso múltiple al canal y transformar los sistemas analógicos a digitales para darle cabida a más usuarios. Para separar una etapa de la otra, a la telefonía celular se ha categorizado por generaciones. A continuación se describen cada una de ellas.

La primera generación (1G)

La 1G de la telefonía móvil hizo su aparición en 1979, se caracterizó por ser analógica y estrictamente para voz. La calidad de los enlaces de voz era muy baja, baja velocidad, la transferencia entre celdas era muy imprecisa, tenían baja capacidad (basadas en FDMA, Frequency Division Multiple Access) y la seguridad no existía. La tecnología predominante de esta generación es AMPS (Advanced Mobile Phone System).

La segunda generación (2G)

La 2G arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad. Las tecnologías predominantes son: GSM (Global System for Mobile Communications); IS-136 (conocido también como TIA/EIA-136 o ANSI-136) y CDMA (Code Division Multiple Access) y PDC (Personal Digital Communications), éste último utilizado en Japón.

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (Short Message Service]. La mayoría de los protocolos de 2G ofrecen diferentes niveles de encriptación. En los Estados Unidos y otros países se le conoce a 2G como PCS (Personal Communications Services).

La generación 2.5G

Muchos de los proveedores de servicios de telecomunicaciones (carriers) se moverán a las redes 2.5G antes de entrar masivamente a 3G. La tecnología 2.5G es más rápida y más económica para actualizar a 3G.

La generación 2.5G ofrece características extendidas para ofrecer capacidades adicionales que los sistemas 2G tales como GPRS (General Packet Radio System), HSCSD (High Speed Circuit Switched Data), EDGE (Enhanced Data Rates for Global Evolution), IS-136B, IS-95B, entre otros. Los carriers europeos y de Estados Unidos se moverán a 2.5G en el 2001. Mientras que Japón ira directo de 2G a 3G también en el 2001.

La tercera generación (3G)

La 3G es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos. Los protocolos

empleados en los sistemas 3G soportan más altas velocidades de información enfocados para aplicaciones mas allá de la voz tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet, sólo por nombrar algunos. Se espera que las redes 3G empiecen a operar en el 2001 en Japón por NTT DoCoMo, en Europa y parte de Asia en el 2002, posteriormente en Estados Unidos y otros países.

Los sistemas 3G alcanzaran velocidades de hasta 384 Kbps permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores. Entre las tecnologías contendientes de la tercera generación se encuentran UMTS (Universal Mobile Telephone Service), cdma2000, IMT-2000, ARIB[3GPP], UWC-136, entre otras.

El impulso de los estándares de la 3G está siendo apoyando por la ITU (International Telecomunications Union) y a este esfuerzo se le conoce como IMT-2000 (International Mobile Telephone).

La cuarta generación (4G)

La cuarta generación es un proyecto a largo plazo que será 50 veces más rápida en velocidad que la tercera generación. Se planean hacer pruebas de esta tecnología hasta el 2005 y se espera que se empiecen a comercializar la mayoría de los servicios hasta el 2010.

Conocer cómo han evolucionado las redes inalámbricas de datos está íntimamente relacionado con la evolución de sistemas celulares, muchas veces las empresas prestadoras de servicios son las mismas que desarrollan productos pertenecientes a redes de datos y celulares o bien participan de cerca en grupos de trabajo dedicados a la investigación y desarrollo.

II. Conceptos básicos

Este capítulo es escrito para plantear un contexto sobre el desarrollo de la tesis y así poder hablar de conceptos generales de una forma natural en capítulos adelante.

II.1 Redes de Computadoras.

Una red de computadoras o red informática es un conjunto de dispositivos y/o computadoras conectados a través de un medio físico o inalámbrico y que comparten información (archivos), recursos (impresoras, scanners, etc.) y servicios.

La idea de creación de una red debía entonces de resolver las siguientes cuestiones:

- Evitar la duplicidad de recursos
- Comunicación eficaz
- Administración de la red

Ya que muchas empresas tenían sus propios estándares, las tecnologías eran incompatibles, y era muy difícil que redes distintas se comunicaran entre si, lo que era incómodo por el gasto de dinero que se necesitaba para reemplazar el equipo viejo.

La solución fue la creación de estándares LAN (red de área local). Estos estándares proporcionaban las pautas para la comunicación de dispositivos de distintos fabricantes, pero no solucionaba la comunicación entre distintas LAN, por lo que hubo la necesidad de crear estándares de comunicación a grandes distancias llamados estándares WAN (red de área amplia).

Las redes de computadoras son imprescindibles en la actualidad. Se crean en base a los propósitos y funciones que quieran desempeñar. Los tipos de redes se pueden clasificar de acuerdo a su arquitectura (topología), tamaño (alcance), direccionalidad de los datos (simples, duplex, full duplex), por relación funcional (peer to peer, cliente servidor), etcétera y tienen características especiales (velocidad de transmisión, número de usuarios, dispositivos empleados, tecnologías, estándares).

Una de las principales clasificaciones que veré en este trabajo es la *Clasificación de las redes en base a su tamaño*, existen muchas definiciones de subconjuntos de redes las cuales fueron creadas por distintos autores, algunos ejemplos son los siguientes:

- DAN - Departamental Area Network (Red de área departamental)
- LAN – Local Area Network (Red de área local)
- CAN – Campus Area Network (Red de área de Campus)
- MAN – Metropolitan Area Network (Red de área metropolitana)
- WAN – Wide Area Network (Red de área amplia)

De acuerdo a CISCO (compañía más importante a nivel mundial desarrolladora de dispositivos de redes de datos), la clasificación de las redes de acuerdo a su tamaño se puede efectuar en tres principales ramas:

LAN (Local Area Network)

Redes de Área Local. Son redes privadas localizadas en un espacio físico pequeño (edificio, empresa). Su extensión máxima es de algunos kilómetros. Muy usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta

velocidad y topología. Son siempre privadas. Están constituidas por computadoras, tarjetas de interfaz de red, dispositivos periféricos, medios de red y dispositivos de red.

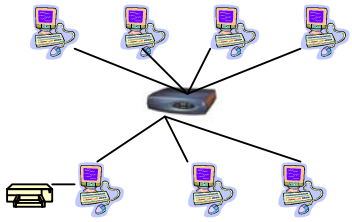


Figura 1. Red de Área Local

Ejemplo: IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring)

MAN (Metropolitan Area Network)

Redes de Área Metropolitana. Las MAN son redes que conectan a las LAN separadas por distancia en un medio geográfico común. Un ejemplo muy claro es una empresa que tiene muchas sucursales. Normalmente un proveedor de servicios conecta dos o más sitios LAN utilizando líneas de comunicación privadas: servicios ópticos o inalámbricos. Actualmente los anchos de banda ópticos son más rentables que las comunicaciones inalámbricas.

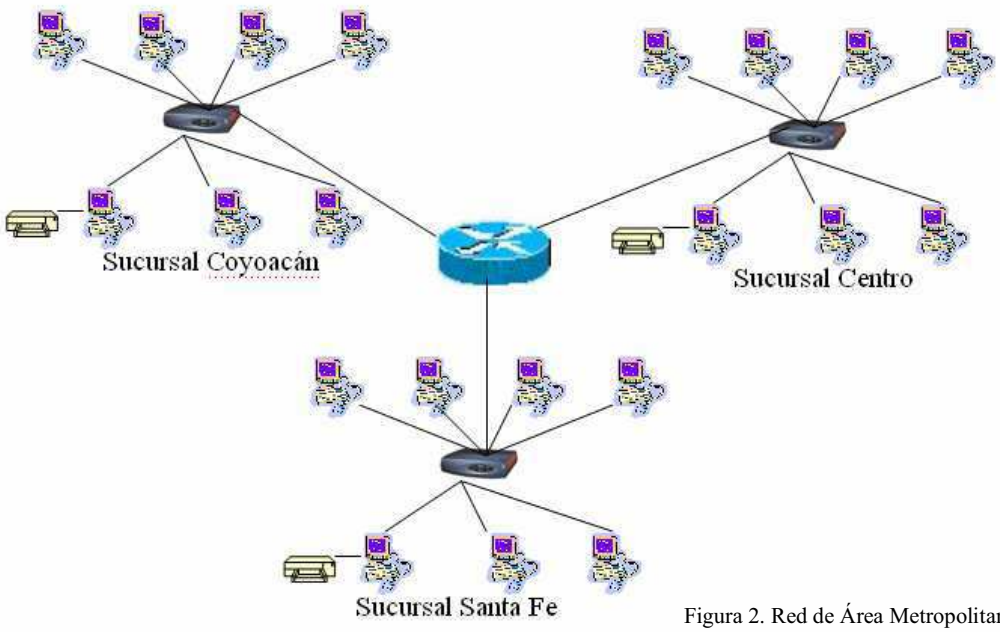


Figura 2. Red de Área Metropolitana

Básicamente son una versión más grande de una Red de Área Local y utiliza normalmente tecnología similar. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. Una MAN tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño. La razón principal para distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Redes de Área Local.

Ejemplo: DQDB, FDDI, ATM, N-ISDN, B-ISDN

WAN (Wide Area Network)

Redes de Amplia Cobertura: Son redes que cubren una amplia región geográfica, a menudo comunican estados, un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system). Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred es transportar los mensajes de un host a otro. En este caso los aspectos de la comunicación pura (la subred) están separados de los aspectos de la aplicación (los host), lo cual simplifica el diseño.

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (Conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

Ejemplo: X.25, RTC, ISDN, etc.

Las oportunidades de trabajo se encuentran en cualquiera de las clasificaciones anteriores, ya que cada una de ellas es un mundo y se requiere más que un curso para aprender a fondo lo que sería pertinente a cada una de ellas.

II.2 Redes Inalámbricas

Las redes inalámbricas son un tipo de redes de datos las cuales plantean una forma de mantener comunicados a los usuarios dentro de un espacio limitado por un medio o canal de transmisión no guiado (aire).

Las redes LAN inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables. Existen numerosos escenarios en los que este hecho puede ser de interés; entre ellos, se pueden citar los siguientes.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 22 MB.

Muchos proveedores de infraestructura están dotando de cable zonas públicas de todo el mundo. En los próximos 12 meses, la mayoría de los aeropuertos, centros de conferencias y muchos hoteles proporcionarán acceso de 802.11b a sus visitantes.

Ventajas de la transmisión inalámbrica

- Movilidad
- Ahorro de dinero y tiempo para la instalación (en comparación con una red cableada: par trenzado, cable, fibra óptica, etc.)
- Escalabilidad
- Seguridad (lugar geográfico, cobertura)

Desventajas

- Tasa de transmisión menor que una red cableada (hasta ahora)
- Seguridad (lugar geográfico)
- Cifrado de datos es requerido, así como autentificación del usuario.
- Recursos limitados (ancho de banda)
- Tasas de errores mayores
- Limitación de potencia para dispositivos inalámbricos
- Factores del medio ambiente que influyen en la transmisión
- Factores de movilidad de usuario que influyen en la transmisión (usuarios caminando, usuarios en un carro a 100km/hr)
- Las velocidades estandarizadas raramente se pueden alcanzar

En general cuando hablamos de redes inalámbricas vienen a la mente dispositivos de transmisión y/o recepción móviles. Un usuario espera maravillas de una red inalámbrica; que se tenga en cualquier lugar (casa, oficina, carro, metro, montaña, etc.), a cualquier hora, cualquier dispositivo (Laptop, PDA, celular, etc.) y uso de cualquier servicio (datos, voz, video) para lo que se necesitan tasas de transmisión adecuadas y el usuario esperaría que fueran sobradas, pero a un precio accesible o barato. Desgraciadamente las condiciones naturales impiden que todas estas características citadas anteriormente para una red inalámbrica se cumplan, por lo que sólo es un ideal.

Existen soluciones apropiadas a las necesidades que un conjunto de personas pueda generar; es decir, hay diferentes tecnologías caracterizadas por la velocidad de transmisión, el número de usuarios que soportan, el costo, la obertura, seguridad, etc.

II.3 El Espectro electromagnético

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio. Los factores que permiten optimizar la capacidad de comunicación dentro de una área geográfica y del espectro de ancho de banda, son considerados más importantes que la forma de como son implementadas.

Las ondas electromagnéticas cubren una amplia gama de frecuencias o de longitudes de ondas y pueden clasificarse según su principal fuente de producción. La clasificación no tiene límites precisos.

Región del espectro	Intervalo de frecuencias (Hz)
Radio-microondas	$0\text{-}3.0\cdot10^{12}$
Infrarrojo	$3.0\cdot10^{12}\text{-}4.6\cdot10^{14}$
Luz visible	$4.6\cdot10^{14}\text{-}7.5\cdot10^{14}$
Ultravioleta	$7.5\cdot10^{14}\text{-}6.0\cdot10^{16}$
Rayos X	$6.0\cdot10^{16}\text{-}1.0\cdot10^{20}$
Radiación gamma	$1.0\cdot10^{20}$-….

Tabla 1. Frecuencias del espectro Electromagnético

Fuente: Leonberger. *Revealing the small range of radio-microwave frequencies*. Phys. Educ. Vol. 37, September 2002, pp. 425-427

II.4 México y las telecomunicaciones

El espectro electromagnético es un recurso limitado, decretado en México como un recurso de todos los mexicanos, administrado por el gobierno federal a través de la Secretaría de Comunicaciones y Transportes en un documento llamado CUADRO NACINAL DE ATRIBUCIÓN DE FRECUENCIAS (1999), el cual indica cómo se debe utilizar el espectro para su mejor aprovechamiento. La Secretaría, entonces, tiene las facultades de atribución, asignación, planificación y ordenamiento.

De acuerdo con el cuadro, el espectro radioeléctrico se divide *en uso libre, usos determinados, uso oficial, usos experimentales y espectro reservado. El espectro para usos determinados se otorga únicamente mediante licitación pública, resultando un proceso muy complejo para ciertos servicios.*

En México, la gestión del espectro radioeléctrico es mala (copia a la FCC en EU, sin atender a las necesidades de nuestro país), casi no se toma en cuenta a la investigación, las bandas de uso libre son pocas y las licitaciones tienen periodos de vida de décadas, por no decir que algunas de ellas siguen fines políticos.

II.5 Proyecto NGN

Next Generation Network (Red de siguiente generación) es una arquitectura de red orientada a reemplazar las redes telefónicas conmutadas de telefonía para servicios de voz y multimedia. Esta arquitectura reúne en un solo sistema todas las tecnologías pertenecientes a las redes de voz y datos para uniformizar en una sola plataforma los servicios y aplicaciones para brindar al usuario servicios y alcanzar una meta como es *la sociedad de la información*. Particularmente adopta del concepto VoIP (Voice over IP) para implementar el acceso al cliente y el trunking de voz por IP (Internet Protocol) o VoATM cuando se trata de una red ATM.

NGN es un modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación (comunicaciones VoIP de nueva generación, videocomunicación, mensajerías integradas multimedia, integración con servicios IPTV, etc.) así como la evolución, migración en términos mas o menos de sustitución o emulación de los actuales servicios de telecomunicación.

Como probablemente se sabe este modelo de referencia puede sintetizarse en el siguiente decálogo de puntos:

- Arquitectura de red horizontal basada en una división diáfana de los planos de transporte, control y aplicación.
- El plano de transporte estará basado en tecnología de conmutación de paquetes IP/MPLS.
- Interfaces abiertas y protocolos estandarizados.
- Migración de las redes actuales a NGN.
- Definición, provisión y acceso a los servicios independiente de la tecnología de la red.
- Soporte de servicios de diferente naturaleza: real time/ non real time, streaming (fluido), servicios multimedia (voz, video, texto).
- Calidad de servicios garantizada extremo a extremo.
- Seguridad.
- Movilidad generalizada.

En México este concepto es relativamente nuevo y no se le ha otorgado la importancia que merece, es decir, si se tiene una red en la cual los servicios estén totalmente integrados sobre una misma plataforma se podrán simplificar procesos, ahorrar costos de mantenimiento, aumentar servicios sin buscar el hilo negro al tratar de integrarlos, y otras grandes ventajas para las empresas y finalmente usuarios, porque se abrirán muchos servicios y el usuario podrá elegir entre ellos.

III. Las tecnologías de comunicación inalámbrica

III.1 Introducción

Las señales inalámbricas son ondas electromagnéticas que pueden viajar a través del vacío del espacio exterior o a través del aire. No se necesitan medios para guiarlas. Las transmisiones inalámbricas pueden cubrir grandes distancias utilizando señales de alta frecuencia. Cada señal utiliza frecuencias diferentes medidas en Hertz, y a su vez cada señal en distinta frecuencia tendrá características diferentes a otra con otra frecuencia.

Cada tipo de comunicación inalámbrica tiene sus ventajas y sus inconvenientes, ya que dependerá de las características que la frecuencia otorgue, a continuación se muestran de forma muy superficial algunas de las características que tienen las frecuencias utilizadas.

Infrarrojo (IR). Tasa de datos muy alta a un costo bajo, aunque la distancia es muy corta. Tendiente a desaparecer o a limitar su crecimiento por su competencia bluetooth.

Banda estrecha. Tasa de datos baja y coste medio. Requiere una licencia y cubre una distancia limitada.

Espectro disperso (SS por sus siglas Spread Spectrum). Coste medio y tasas de datos altas. Limitado a cubrir un campus.

Servicio de Comunicaciones Personal de Banda Ancha (PCS, Personal Communication Service). Tasas de datos bajas, coste medio y cubre el área de una ciudad.

Circuito y datos de paquetes (datos celulares y datos de paquetes digitales celulares CDPD Cellular Digital Packet Data). Tasas de datos bajas, cuotas altas por paquete, cobertura nacional.

Satélite. Tasas de datos bajas, alto costo, cobertura nacional o mundial.

III.2 Clasificación de las redes inalámbricas

Como ya he mencionado, existen diferentes clasificaciones de las redes, por lo que también existen diferentes clasificaciones de las redes inalámbricas. En este ensayo abordaré la principal clasificación manejada a nivel mundial, que es por alcance, sin dejar de tomar en cuenta que podrían existir clasificaciones en base a frecuencia, número de usuarios, seguridad, etc.

En la clasificación de redes inalámbricas por alcance, básicamente se parte de la clasificación de redes, tomando como referencia a las LAN, WAN y MAN, sin embargo entran otras ramas que son vitalmente importantes por el desarrollo de tecnología y necesidades en usuarios que en un mundo donde la información actualizada minuto por minuto es el pan de cada día para la toma de decisiones correctas.

Para una mayor comprensión, veamos el tipo de dispositivos que suelen interactuar en las redes, mostrados en la siguiente figura:

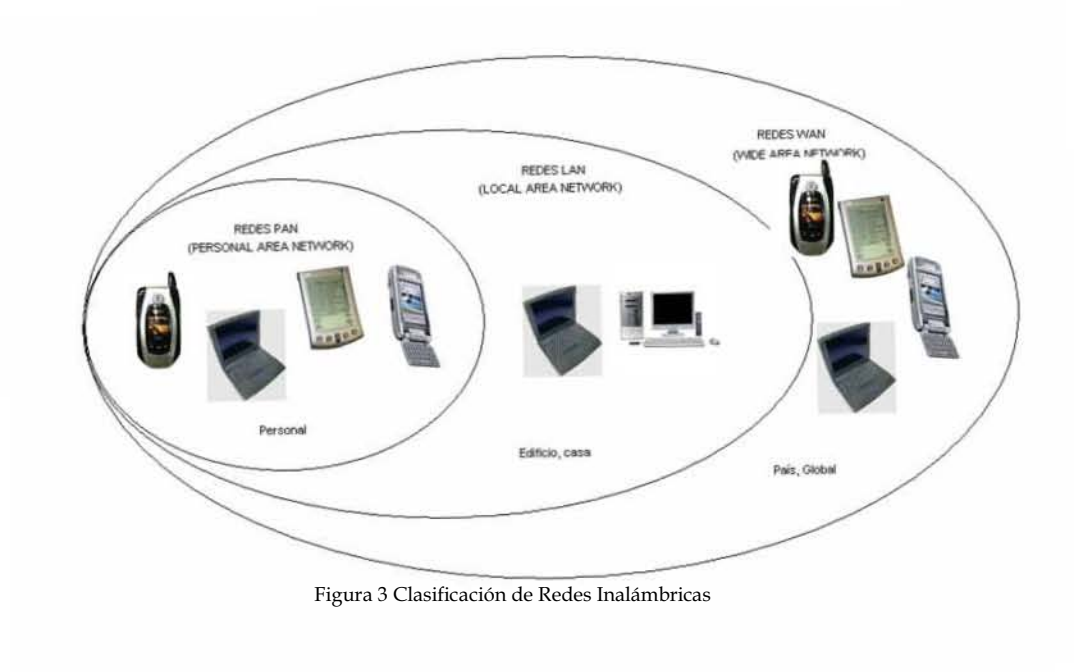


Figura 3 Clasificación de Redes Inalámbricas

PAN. Personal Area Network (Red de área personal).

Una PAN es un tipo de red compuesta de dos o más dispositivos que mantienen una comunicación, limitada por pocos metros. Este tipo de redes alimenta las necesidades de usuarios que cuentan con un dispositivo y desean transmitir datos con algún otro dispositivo o periférico cercano sin necesidad de conectarlos entre sí.

Este tipo de redes se caracterizan por una menor potencia de transmisión-recepción, rango corto, comunicación de dos vías (dúplex). Las tecnologías más importantes que se han desarrollado para esta necesidad son Bluetooth, Infrarrojo (IR), ZigBee, etcétera; y las aplicaciones suelen ser de diversa índole: para reemplazar los cables de los periféricos en una computadora, transmitir imágenes o sonido entre dispositivos (o bien videos cortos), pago electrónico de boletos (en E.U., Japón, Europa y algunos países desarrollados), dispositivos para estacionarse, etc.

WLAN Wireless Local Area Network (Red de área local inalámbrica)

Reemplazan y comparten las funciones de las LAN. Son funcionales porque permiten eliminar o reducir la infraestructura y tienen gran adaptabilidad, son cómodas porque no tienen cables y permiten al usuario moverse libremente dentro del rango de cobertura, que usualmente es de hasta algunos cientos de metros en espacio libre sin fronteras ni obstáculos.

Este rango de cobertura varía dependiendo del equipo utilizado, la frecuencia en la que trabaja, el lugar donde se implementa, algunos parámetros naturales, las antenas utilizadas, la velocidad a la que se viaja dentro del rango de cobertura, etc. Generalmente para un espacio a puerta cerrada, por ejemplo un piso de un edificio, un Access Point que cuente con el estándar 802.11b, muy popular para redes inalámbricas actualmente (más adelante explicaré los distintos estándares y el organismo que los determina, la IEEE), la cobertura promedio suele ser de alrededor de 100 metros.

Este tipo de redes son exitosas en el mercado, además de que su popularidad va en aumento, por lo que dispositivos de conexión inalámbrica (tarjetas) han sido incorporadas en muchas Lap Top´s como equipamiento estándar y no adicional.

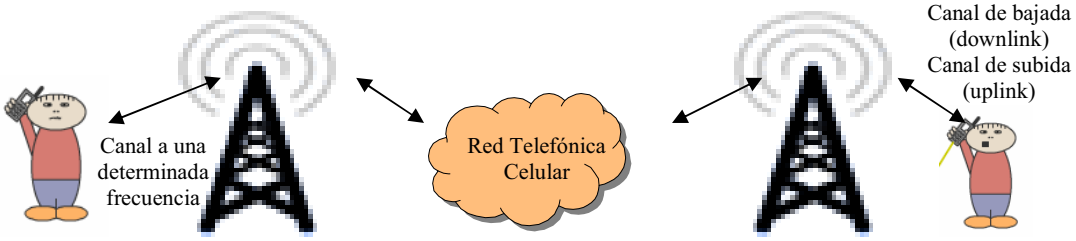
WWAN Wireless Wide Area network (Red de área amplia inalámbrica)

Difiere de la WLAN porque el rango de cobertura es mayor. Se utilizan tecnologías celulares y satelitales para ofrecer servicios inalámbricos de coberturas tan grandes. Generalmente este tipo de coberturas se ofrecen de forma regional, nacional, continental o hasta global por un proveedor de servicio o una compañía grande (llamadas Carriers´s). Actualmente las nuevas computadoras cuentan con capacidades integradas para conectarse a una red WWAN, lo que significa que cuentan con tarjetas que trabajan a frecuencias específicas que permitirán al usuario recibir o mandar datos.

Este tipo de red inalámbrica permite que los usuarios tengan una movilidad más grande que con una WLAN, suele utilizarse para usuarios de negocios o técnicos que ofrecen su servicio en distintas partes. Permite que estas personas cuenten con aplicaciones o servicios de Internet (como e-mail, FTP, Telnet, etc) aún si están fuera de su oficina.

Wireless WAN usa las redes celulares para la transmisión de datos (la información es de diferente naturaleza, la infraestructura estaba diseñada para la transmisión de voz, ver siguiente capítulo). La siguiente figura muestra la forma en que un dispositivo celular transmite información a una torre estación base vía ondas de radio. Diferentes tecnologías pueden usar diferentes frecuencias.

Figura 4. Comunicación Celular



En este primer acercamiento a una red celular vemos cómo se efectúa la comunicación entre dos dispositivos, por medio de una estación base que asigna un espacio al teléfono para que pueda llamar a su amigo, sin embargo, los detalles de la Red Telefónica Celular todavía no son detallados

Este tipo de redes usan la infraestructura celular existente, por lo que cuentan con opción de transmitir datos o emitir llamadas de voz simultáneamente sobre la misma red. Es por eso que aparatos celulares y tarjetas WWAN tienen la habilidad de hacer llamadas y recibir datos, porque el sistema se los permite.

Entre las tecnologías que encontramos en esta clasificación se encuentran WiMax, UMTS, SMS, GPRS, CDMA, CDPD, WIFi, LMDS, etc

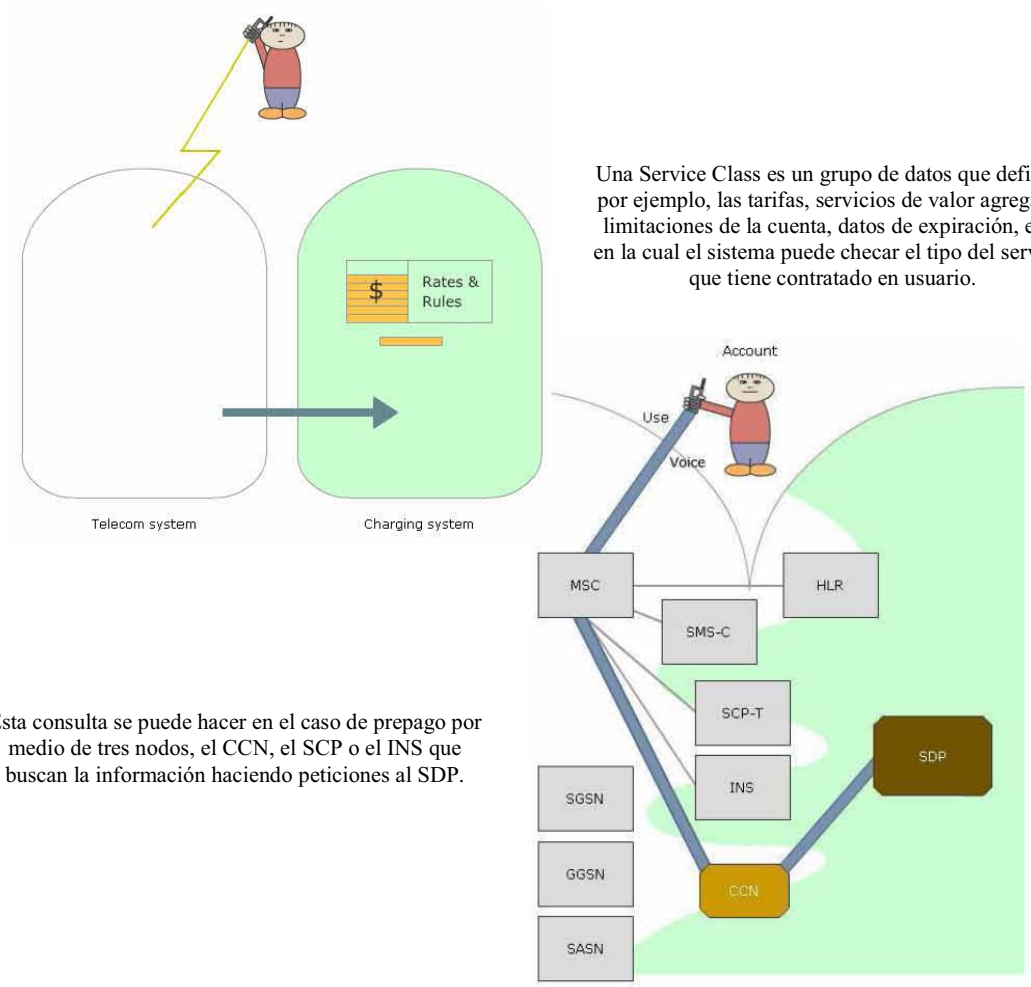
Entonces, recapitulando las dos clasificaciones de redes inalámbricas que se tienen nos damos cuenta de que son similares, permiten a un usuario acceder a la información de forma inalámbrica en una PC o una PDA, pero los usos son distintos al igual que las aplicaciones que están destinadas a cumplir.

Podría pensarse que tecnologías que pertenecen a WLAN están peleadas por el mercado de las tecnologías de WWAN, pero cada una tiene a sus consumidores bien definidos y es posible trabajar con las dos al mismo tiempo sin que afecte su funcionamiento tomando las consideraciones necesarias.

Redes Celulares

Las redes celulares varían dependiendo del Carrier (el que brinda el servicio) y el fabricante de elementos de red (por ejemplo Ericsson, Nokia, Nortel, etc.). También dependerá la llamada si se efectúa por medio de pre o post pago tendrá distintos caminos, al igual si es larga distancia nacional, internacional, etc; es decir, varía de acuerdo a múltiples condiciones y necesidades. En el siguiente ejemplo muestro de una forma muy superficial el funcionamiento de la Red Telefónica Celular y de la red de Cobro, especificado para el área de prepago.

- La cuenta se inicializa, los precios y las reglas se crean y las tarjetas SIM son distribuidas a un revendedor.
- El subscriptor compra la cuenta con el revendedor.
- El subscriptor activa la cuenta usando, generalmente un servicio de voz o bien, la cuenta ya viene activada.
- El subscriptor quiere hacer una llamada; en el momento en que abre el teléfono, el sistema de Telecom le asigna una canal.
- Cuando el usuario está llamando a otro usuario, el sistema de telecomunicaciones hace una petición al MSC (Master Switch Control), para el cargo en tiempo real, el MSC delega el control al SCP (Service Control Point)
- Hay tres nodos que implementan esta función
- El CCN (Charging Control Node) inicia la interacción al SDP (Service Data point)
- El SDP contiene a todos los subscriptores, cuentas y tarifas, es el encargado de bloquear en caso de que no tenga suficiente dinero o reservar un poco para la llamada.



Una Service Class es un grupo de datos que definen, por ejemplo, las tarifas, servicios de valor agregado, limitaciones de la cuenta, datos de expiración, etc., en la cual el sistema puede checar el tipo del servicio que tiene contratado en usuario.

Esta consulta se puede hacer en el caso de prepago por medio de tres nodos, el CCN, el SCP o el INS que buscan la información haciendo peticiones al SDP.

Figura 5. Service Class y Nodos de la Red Celular

- Una vez que el sistema ha aprobado que el subscriptor tiene dinero para realizar la llamada, se buscan los datos del teléfono B en la HLR (Home Location Register), el cual contiene información de dónde se puede localizar al usuario.
- Se enruta la llamada
- Se establece la comunicación
- Se termina la llamada y se envía la información de cobro al SDP, se regresan los minutos que estaban reservados y no fueron ocupados.

Comparativa entre WLAN y WWAN

Esta comparativa se centrará en cinco puntos que son considerados importantes en el desarrollo y la planificación de redes inalámbricas:

Cobertura
Por definición WLAN opera en un área local pequeña, aproximadamente de 100 metros. Son típicamente usadas en edificios para reemplazar una red cableada tipo Ethernet, o en una casa para permitir que muchos usuarios accedan a Internet.

WWAN cubre un área "amplia" como la que cubren los sistemas celulares. Se tiene información sin importar el lugar donde se encuentre, lo cual es una muy buena ventaja sobre WLAN.

Velocidad (tasa de transmisión, thoughput)
Existen diferentes velocidades para las WLAN, en este cuadro se distinguen algunas

Estándar	Velocidad máxima
802.11b	11 Mbps
802.11a	54 Mbps
802.11g	54 Mbps
802.11n	600 Mbps

Tabla 2. Velocidad Máxima en Mbps contra estándar utilizado

Aunque la velocidad máxima estipulada es alta para algunos estándares la velocidad típica puede decrementarse demasiado, dependiendo de factores que influyen en la propagación, la distancia, y el número de usuarios conectados a un mismo AP. Por ejemplo, aunque la velocidad máxima para el estándar sea de 11 Mbps, la típica anda entre 1 y 4 Mbps, sin embargo la velocidad no es el verdadero problema con ellas, ya que como vemos, estándares recientes alcanzan velocidades superiores.

Un problema potencial es la saturación del canal, es decir, si muchas personas o negocios usan redes inalámbricas en estos canales en un área contigua tal que los AP compartan el mismo rango de transmisión pueden saturar el lugar donde ellos están transmitiendo, en otras palabras las señales se interferirán (interferencia es un tema abordado en el capítulo III.3).

La velocidad de una WWAN difiere según la tecnología que se use. Por ejemplo las redes con tecnología GPRS ofrecen una velocidad máxima al usuario de 115 kbps, si ocho time slots en una célula son dedicados a la transmisión de datos (un time slot puede proveer entre 9 y 21 kbps). Una tasa realista puede oscilar entre 30 y 50 kbps, se puede decir que esta tasa crecerá en el futuro.

La tasa de transmisión en CDMA tuvo velocidades iniciales de 14.4kbps, pero ha crecido a un máximo de 153 kbps, si los carriers implementan la tecnología de redes CDMA2000 1x. Esto brinda a los usuarios velocidades típicas de 40 a 70kbps.

Futuras redes inalámbricas WAN podrán utilizar tasas mayores a los 2Mbps en un canal estándar de CDMA de 1.25MHz. Estas tecnologías son CDMA2000 1xEV-DO y WCDMA también conocida como UMTS.

Seguridad
La seguridad es uno de los aspectos más importantes al usar una red inalámbrica.

Se considera a la seguridad una principal ventaja de las redes celulares (WWAN) en comparación a las redes WLAN, en donde la seguridad es uno de los aspectos más débiles.

Por ejemplo el estándar 802.11b tiene muchas capas de seguridad, sin embargo existen debilidades en todas estas capas, mientras que en las redes celulares se ha incorporado tecnología militar además de una encripción y autenticación sofisticada.

La seguridad será un punto tocado más a fondo en el capítulo III.12.

Costo

Las redes LAN inalámbricas operan en un rango de frecuencias que no necesitan licencia. No hay costo de servicio extra por usar una red privada LAN (como las que son incorporadas en casas y oficinas). Habrá un costo mensual si esta red inalámbrica quiere salir a Internet y será pagado al proveedor de servicio. EL costo real involucrará factores como el cableado, el dispositivo (AP), mantenimiento, y las tarjetas inalámbricas para los equipos remotos.

Para las redes WWAN, la red inalámbrica actúa como un proveedor de servicio de Internet, pero bajo su propia red. El costo mensual de este servicio es similar al costo mensual por servicio telefónico. Se puede pagar por un tiempo determinado o por Megabite transferido.

III.3 Canal Inalámbrico

Hasta ahora hemos visto algunos antecedentes indispensables. Las frecuencias utilizadas por los dispositivos están controladas por los organismos reguladores de cada país y por organismos reguladores de las telecomunicaciones a nivel continental e internacional. Estas frecuencias se encuentran en la banda de radio, es decir de los 3kHz a los 300 GHz, dependiendo de la frecuencia, como hemos venido manejando, se tendrán parámetros naturales que distorsionarán y atenuarán la señal en un receptor.

Para comprender la transmisión de datos se han planteado distintos modelos matemáticos que ayudan a la comprensión y explican algunos fenómenos según la complejidad de lo que queramos representar. Estos modelos serán veremos adelante en el capítulo de propagación.

Entre los factores físicos y naturales que determinan la propagación de una onda electromagnética encontramos ruido, atenuación, interferencia, bloqueos, efectos de "multipath fading", además de prever que los usuarios son móviles y no siempre se moverán en una dirección a velocidad constante. Las características que he mencionado imponen los límites fundamentales de rango, velocidad de transmisión y reliabilidad de líneas de transmisión inalámbricas.

Se tiene entonces el siguiente esquema para ejemplificar lo anterior:

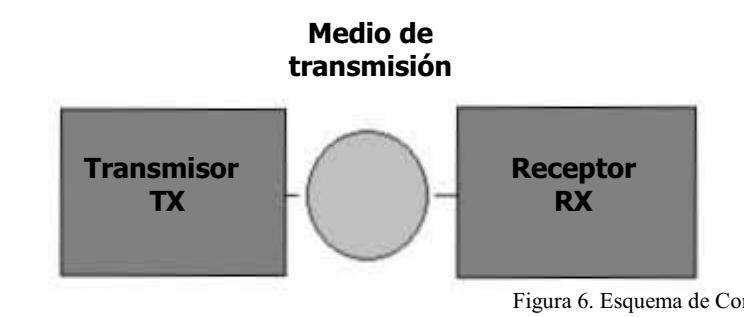


Figura 6. Esquema de Comunicación I

La señal de radio puede ser severamente dañada o distorsionada al llegar al receptor, hasta el punto que no se pueda recuperar y la comunicación se pierda. En este capítulo veremos cuáles son los principales factores físicos y naturales por los cuales una comunicación puede perderse, o bien que la señal transmitida sea modificada para después poder explicar los modelos que han planteado para la propagación de ondas de radio.

Los factores adversos al canal de radio entonces son:

- Ruido
- Pérdidas por trayectoria
- Desvanecimientos
- Interferencia

Ruido

El ruido es una perturbación o una señal anómala. Esta señal se caracteriza porque no es deseada en un sistema de transmisión, recepción o de comunicaciones. El ruido se encuentra en todas las frecuencias, es parte del canal inalámbrico.

El ruido blanco, denominado así por la asociación de la luz blanca, se caracteriza por su distribución uniforme en todo el espectro; es decir, es un ruido cuya respuesta en frecuencia es plana, lo que significa que su amplitud para todas las frecuencias es plana.

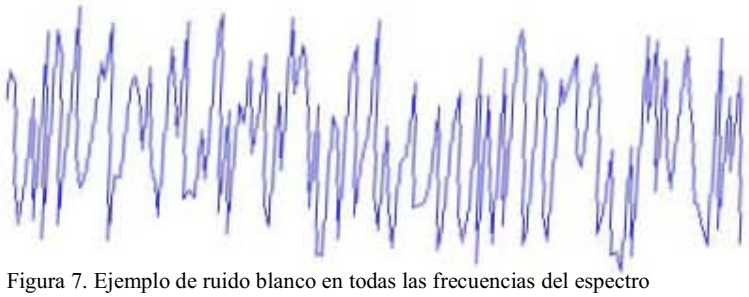


Figura 7. Ejemplo de ruido blanco en todas las frecuencias del espectro

Pérdidas por trayectoria

Existen diferentes maneras de modelar a las señales de esta naturaleza:

- ***El modelo de la óptica geométrica.***

En este modelo, la señal tiene una propagación como una línea recta infinitamente delgada, ignora la existencia de los campos eléctrico y magnético y su carácter vectorial.

- ***Teoría electromagnética.***

Descrito y difundido por Maxwell, realizando una síntesis sobre los trabajos de Ampere y Faraday sobre la electricidad y el magnetismo, dando origen a las ondas electromagnéticas (entre ellas la luz).

Esta teoría absorbe a la óptica geométrica, ya que en realidad la línea recta será el vector de *Pointing* (vector con el que se obtiene la dirección de propagación). Después de que Maxwell planteara sus ecuaciones Hertz realizó experimentos en los cuales se proponía indagar sobre la existencia de estas ondas electromagnéticas, verificando la teoría de Maxwell.

A partir de los trabajos de Maxwell y Hertz se da inicio a una revolución en las comunicaciones inalámbricas.

Mecánica cuántica.

Es una teoría que aplica las reglas cuánticas de los campos continuos de la física. En el campo electromagnético da una explicación entre la interacción de este campo con el resto de la materia, llamada electrodinámica cuántica, es decir, describe todos los fenómenos que implican las partículas eléctricamente cargadas que obran recíprocamente por medio de la fuerza electromagnética y se la ha llamado "la joya de la física" por su predicción extremadamente exacta de cantidades como el momento magnético anómalo del electrón y el salto de Lamb en el nivel de energía del hidrógeno. Físicamente, esto se traduce al marco de partículas cargadas (y de sus antipartículas) que interactúan por el intercambio de fotones. Estas interacciones se pueden describir pictóricamente con diagramas de Feynman, y QED (por "*Quantum Electro Dynamics*") fue históricamente la teoría a la cual los diagramas de Feynman se aplicaron primero.

QED fue la primer teoría cuántica del campo en la cual las dificultades para construir una descripción completa de campos y de creación y aniquilación de partículas cuánticas, fueron resueltas satisfactoriamente.

Conclusión parcial:

La óptica geométrica es una versión simplificada de la teoría electromagnética, ya que cuando una estructura es grande en términos de λ, los resultados no varían mucho y puede usarse con muy buena aproximación; sin embargo si lo que se busca es mucha exactitud se deberá utilizar un modelo que satisfaga el grado de aproximación adecuado.

En esta tesis utilizaré el modelo de la óptica geométrica y algunas veces el modelo de la teoría electromagnética ya que nos permiten explicar fácilmente el tema que se desarrolla y satisface las necesidades de aproximación que no son extremadamente exigentes. Para una mayor comprensión de lo que ocurre en el medio, los parámetros que tendremos que considerar se facilita la siguiente tabla comparativa entre los modelos de óptica geométrica y la teoría electromagnética.

Óptica geométrica	**Teoría electromagnética**	**Teoría electrodinámica cuántica**
η – índice de refracción	Eo	E – Energía de un fotón
v – velocidad a la que se propaga una onda en el medio	E	h – constante de Planck
c – velocidad de la luz	M	Frecuencia de la onda en Hertz
	M	
	Σ	

Tabla 3. Parámetros utilizados en la óptica geométrica, la teoría electromagnética y la teoría electrodinámica cuántica

Tomando el cuenta al modelo de óptica geométrica

La ley de Snell es una fórmula simple utilizada para calcular el ángulo de refracción de la luz al atravesar la superficie de separación entre dos medios de índice de refracción distinto. El nombre proviene de su descubridor, el matemático holandés Willebrord Snell van Royen (1580-1626).

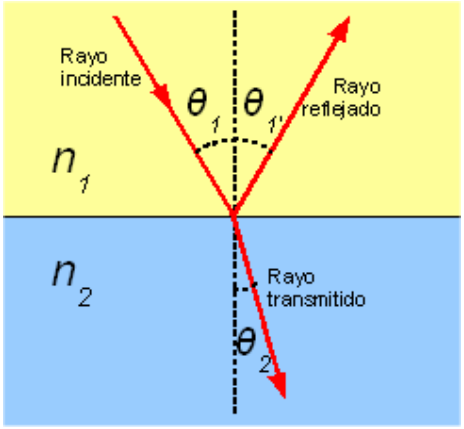


Figura 8. La Ley de Snell, donde se puede observar claramente al rayo incidente, la desviación que ocurre en el rayo transmitido y el rayo reflejado.

La ley de Snell dice que el producto del índice de refracción por el seno del ángulo de incidencia es constante para cualquier rayo de luz incidiendo sobre la superficie separatriz de dos medios. Aunque la ley de Snell fue formulada para explicar los fenómenos de refracción de la luz se puede aplicar a todo tipo de ondas atravesando una superficie de separación entre dos medios en los que la velocidad de propagación la onda varíe.

Consideremos dos medios caracterizados por índices de refracción n_1 y $n_2$separados por una superficie S. Los rayos de luz que atraviesen los dos medios se refractarán en la superficie variando su dirección de propagación dependiendo del ratio entre los índices de refracción n_1 y n_2.

Para un rayo luminoso con un ángulo de incidencia θ_1 sobre el primer medio, ángulo entre la normal a la superficie y la dirección de propagación del rayo, tendremos que el rayo se propaga en el segundo medio con un ángulo de refracción θ_2 cuyo valor se obtiene por medio de la ley de Snell.

$$n_1 \sin\theta_1 = n_2 \sin\theta_2$$

Obsérvese que para el caso de $\theta_1=0$ (rayos incidentes de forma perpendicular a la superficie) los rayos refractados emergen con un ángulo $\theta_2=0$ para cualquier n_1 y n_2.

La simetría de la ley de Snell implica que las trayectorias de los rayos de luz son reversibles. Es decir, si un rayo incidente sobre la superficie de separación con un ángulo de incidencia θ_1 se refracta sobre el medio con un ángulo de refracción θ_2, entonces un rayo incidente en la dirección opuesta desde el medio 2 con un ángulo de incidencia θ_2 se refracta sobre el medio 1 con un ángulo θ_1.

Una regla cualitativa para determinar la dirección de la refracción es que el rayo en el medio de mayor índice de refracción se acerca siempre a la dirección de la normal a la superficie. La velocidad de la luz en el medio de mayor índice de refracción es siempre menor.

La ley de Snell se puede derivar a partir del principio de Fermat, que indica que la trayectoria de la luz es aquella en la que los rayos de luz necesitan menos tiempo para ir de un punto a otro. En una analogía clásica propuesta por el físico Richard Feynman, el área de un índice de refracción más bajo es substituida por una playa, el área de un índice de refracción más alto por el mar, y la manera más rápida para un socorrista en la playa de rescatar a una persona que se ahoga en el mar es recorrer su camino hasta ésta a través de una trayectoria que verifique la ley de Snell, es decir, recorriendo mayor espacio por el medio más rápido y menor en el medio más lento girando su trayectoria en la intersección entre ambos.

Refracción (Refraction)

Se produce cuando la luz pasa de un medio de propagación a otro con una densidad óptica diferente, sufriendo un cambio de velocidad y un cambio de dirección si no incide perpendicularmente en la superficie.

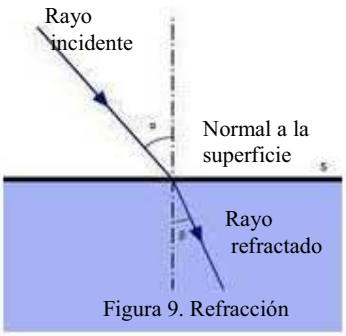


Figura 9. Refracción

Esta desviación en la dirección de propagación se explica por medio de la ley de Snell. Esta ley, así como la refracción en medios no homogéneos, son

consecuencia del principio de Fermat, que indica que la luz se propaga entre dos puntos siguiendo la trayectoria de recorrido óptico de menor tiempo.

Por otro lado, la velocidad de propagación de la luz en un medio distinto del vacío está en relación con la longitud de la onda y, cuando un haz de luz blanca pasa de un medio a otro, cada color sufre una ligera desviación. Este fenómeno es conocido como dispersión de la luz. Por ejemplo, al llegar a un medio más denso, las ondas más cortas pierden velocidad sobre las largas (ej: cuando la luz blanca atraviesa un prisma). Las longitudes de onda corta son hasta 4 veces más dispersadas que las largas lo cual explica que el cielo se vea azulado, ya que para esa gama de colores el índice de refracción es mayor y se dispersa más.

Existen ciertos fenómenos que contradicen la propagación rectilínea de las ondas, los cuales tenemos que considerar para nuestro trabajo:

Difracción

Cuando la luz pasa por aberturas o bordea obstáculos se producen fenómenos que contradicen la propagación rectilínea, estos fenómenos, que aparecen más acentuados a medida que los obstáculos y las aberturas se hacen más pequeños en relación con la longitud de onda de la luz utilizada, constituyen la difracción, y son una consecuencia natural del carácter ondulatorio de la luz.

En física, la difracción es un fenómeno característico de las ondas que consiste en la dispersión y curvado aparente de las ondas cuando encuentran un obstáculo. La difracción ocurre en todo tipo de ondas, desde ondas sonoras, ondas en la superficie de un fluido y ondas electromagnéticas como la luz y las ondas de radio. También sucede cuando un grupo de ondas de tamaño finito se propaga; por ejemplo, por culpa de la difracción, un haz angosto de ondas de luz de un láser deben finalmente divergir en un rayo más amplio a una distancia suficiente del emisor.

El fenómeno de la difracción es un fenómeno de tipo interferencial y como tal requiere la superposición de ondas coherentes entre sí. Los efectos de la difracción disminuyen hasta hacerse indetectables a medida que el tamaño del objeto aumenta comparado con la longitud de onda.

Dispersión (Scattering)

- En matemáticas, dispersión significa el grado de distanciamiento de un conjunto de valores respecto a su valor medio. El término correspondiente en inglés es *dispersion*.

- En física, dispersión es el fenómeno por el cual un conjunto de partículas que se mueve en una dirección determinada rebota sucesivamente con las partículas del medio por el que se mueve hasta perder una dirección privilegiada de movimiento. Por ejemplo, la luz en el cielo se dispersa haciendo que lo veamos azul en vez de negro. El cielo luce porque recibimos radiación dispersada. La traducción al inglés con esta acepción es *scattering*.

¿Cómo afecta el modelo de la óptica geométrica a las comunicaciones inalámbricas?

Dado que hemos definido los fenómenos que describen la trayectoria de una onda por medio de la óptica geométrica veremos el siguiente ejemplo que muestra sus efectos.

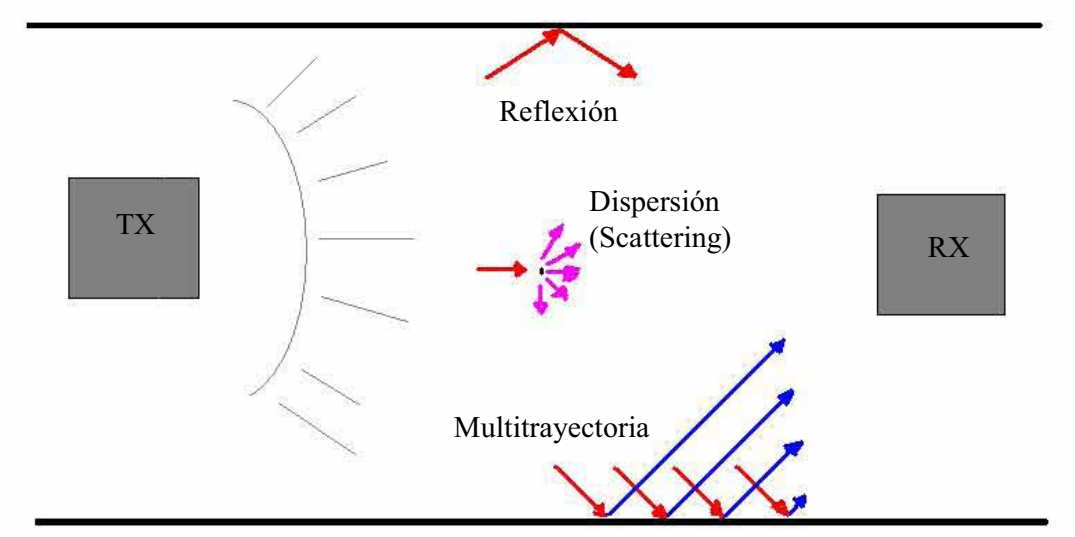


Figura 10. Fenómenos que disminuyen la potencia de la señal en el receptor

Entonces las Pérdidas por trayectoria son la reducción de la potencia de la señal en el receptor en relación con la potencia transmitida, las cuales son proporcionales a la distancia y son debidas a obstáculos entre transmisor y receptor, tales como paredes, pisos, objetos en movimiento, etc. y degradarán la señal a varios grados.

Fluctuaciones y desvanecimientos

Una fluctuación es un cambio, una oscilación y un desvanecimiento es la pérdida de una señal. Hablando de la transmisión y recepción de señales las fluctuaciones se darán por el desvanecimiento de las señales.

Existen diferentes categorías de fluctuaciones, las cuales influyen en la recepción de señales de distintas maneras y son provocadas por distintas razones:

- ***Path lost***: determina cómo la señal recibida promedio disminuye con respecto a la distancia entre transmisor y receptor.
- ***Shadow fading***. (también llamadas distorsiones lentas o “show fading”) este tipo de fluctuaciones caracterizan la atenuación de la señal debido a la disposición del terreno y objetos entre transmisor y receptor (edificios, paredes, etc.).
- ***Raleigh fading***. (llamadas distorsiones rápidas o “fast fading”) caracterizan fluctuaciones rápidas debido a los efectos de múltiples trayectorias. Existen modelos que caracterizan a las fluctuaciones rápidas como Rayleigh y Ricen, los cuales serán estudiados en el subtema de propagación.

Ejemplo de fluctuaciones y desvanecimientos:

Entonces en el receptor se tendrán muchos frentes de onda que contienen la misma información, pero que llegan en tiempos distintos, esto es considerando que el usuario estará siempre en un solo lugar, un buen diagrama que interpreta esta idea es el siguiente:

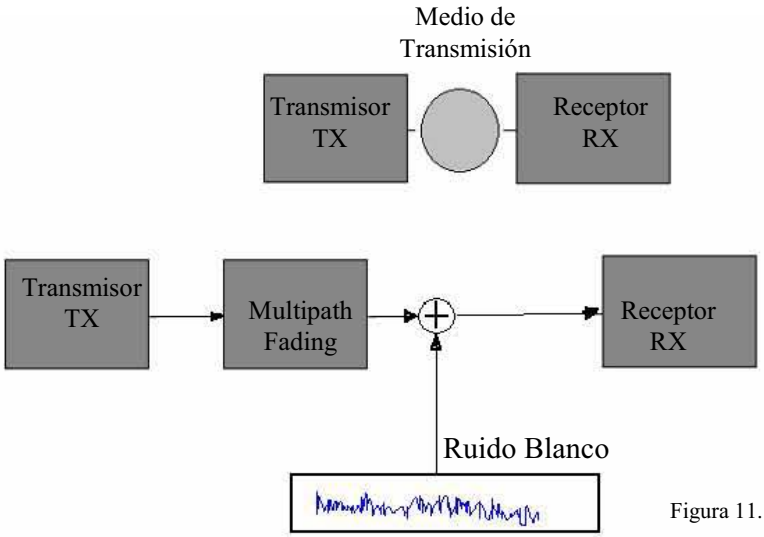


Figura 11. Esquema de Comunicación II

Desvanecimiento en Comunicaciones Inalámbricas (Fading)

En comunicaciones inalámbricas, el desvanecimiento de una señal es causado por el efecto multipath o multitrayectoria. El efecto multipath significa que una señal transmitida desde un transmisor tendrá copias múltiples que atraviesan diferentes trayectorias al llegar al receptor. Entonces, en el receptor, la señal recibida será la suma de todas estas señales de diferente trayectoria. Ya que las trayectorias que atraviesan estas señales son diferentes, algunas llegarán más rápido que otras y otras incluso, se perderán para siempre.

Aquella señal que se encuentre en dirección al origen o transmisor (Línea de campo; el término que se maneja en inglés es Light of signal - LOS) será la que tenga la trayectoria más corta y por consiguiente la más rápida en llegar.

Las señales interactuarán unas con otras, si se encuentran en fase, incrementarán la señal resultante, por otro lado, la señal resultante se minimizará o debilitará si están fuera de fase. A este fenómeno se le llama *fading* (desvanecimiento). En general, existen poscriterios para medir el desvanecimiento de un canal, *Dopper spread* y *Delay spread.*

Dopper spread

Además del efecto Doppler, si un transmisor se mueve en relación al receptor, la frecuencia de la señal será menor que la que en realidad está enviando, o bien la frecuencia será mayor. En comunicaciones inalámbricas, existen muchos factores que pueden causar un movimiento relativo entre el transmisor y el receptor, el cual puede ser el movimiento de un celular, el movimiento de alguno de los objetos contextuales, el cual causará el cambio de distancia de trayectoria entre el transmisor o receptor.

Las distancias que recorren las señales entre receptor y transmisor suelen ser distintas, y corresponderán a los diferentes movimientos de velocidad de las señales transmitidas y a su vez se turnarán en diferentes cambios de frecuencias de las señales. Como resultado, una extensión o ensanchamiento de frecuencia es causada al ver el espectro de la señal.

En relación al Doppler Spectrum Spread (espectro Doppler disperso) existe un concepto llamado coherencia de tiempo, el cual está relacionado al recíproco del doble

del máximo Doppler. El tiempo de coherencia es usado para medir un intervalo de tiempo en el cual una cantidad pequeña de desvanecimiento ocurre, específicamente si la señal banda base varía más rápidamente que el tiempo de coherencia, la distorsión que es causada por efecto Doppler será insignificante. Esta situación es llamada desvanecimiento lento.

De otra forma, si la señal banda base varía más lentamente que el tiempo de coherencia, la distorsión proveniente del efecto Doppler será significante, la cual es llamada *desvanecimiento rápido*.

Delay Spread

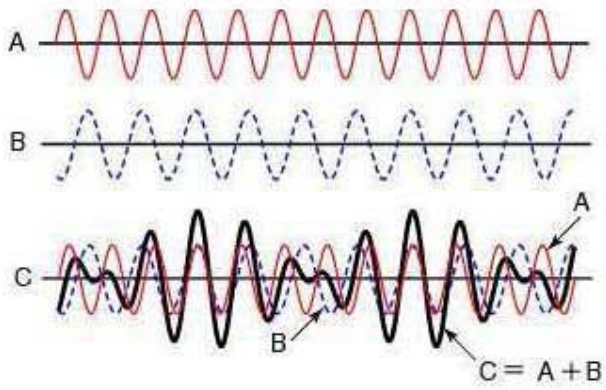
Las diferentes señales entre el transmisor y el receptor corresponden a diferentes tiempos de transmisión. Es decir, si un trasmisor emite una señal pulso o cuadrada, múltiples copias de la señal son recibidas en el receptor en momentos diferentes, pero con intensidades cada vez más bajas. Esto se debe a que las señales que tienen una trayectoria más cercana llegan más rápido que las que tienen que rebotar o tomar una trayectoria distinta.

El efecto directo de estos arribos de señales no simultáneas de la señal original causa un ensanchamiento del espectro, llamada distorsión temporal.

La distorsión temporal agrega una limitante en la capacidad de transmisión máxima en el canal inalámbrico, específicamente, si el periodo de un pulso de datos banda base es más largo que el retraso del espectro, ocurrirá una interferencia entre símbolos (ISI – Inter Symbol Interference). Esto significa que las señales de datos de dos pulsos vecinos serán recibidas al mismo tiempo, lo cual causa que el receptor no sea capaz de distinguir entre estos pulsos.

De acuerdo al concepto de espectro ensanchado, hay un término clave llamado coherencia de banda, usada para medir el límite máximo de transmisión que se puede transmitir por un canal sin interferencia entre símbolos (ISI).
La coherencia de banda es definida como el 10% del recíproco del retraso promedio rms del Delay spread. Si el ancho de banda de la señal de un transmisor es más pequeña que la coherencia del ancho de banda del canal, el canal estará libre de ISI, de otra forma, el canal mostrará un filtro selectivo en frecuencia y sufrirá de ISI.

Figura 12. Efecto de la suma de señales defasadas



En esta figura se intenta mostrar la suma de dos señales que están defasadas, la señal A y la señal B tienen diferentes frecuencias, la suma de ellas causará una señal resultante de una forma peculiar, mientras ambas señales están en fase se incrementa la intensidad o amplitud, pero si están defasadas la amplitud decrece.

III.4 –Modelo de referencia OSI

A finales de la década de los setenta, la Organización Internacional para la Normalización (ISO) empezó a desarrollar un modelo conceptual para la conexión en red al que llamó con el nombre de Open Systems Interconnection Referente Model, o modelo de Referencia de Interconexión de Sistemas Abiertos. En los entornos de trabajo con redes se le conoce comúnmente como modelo de referencia OSI. En 1984, este modelo fue el estándar internacional para las comunicaciones en red al ofrecer un marco de trabajo conceptual que permitía explicar el modo en que los datos se desplazaban dentro de una red.

El modelo OSI divide en siete capas el proceso de transmisión de la información entre equipos informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global. Este marco de trabajo estructurado en capas, aun siendo puramente conceptual, puede utilizarse para describir y explicar el conjunto de protocolos reales que se utilizan para la conexión de sistemas, es decir, existe una capa o suite de protocolos los cuales están organizados najo jerarquías que juntos pueden llevar a cabo una transmisión de datos de un nodo a otro en la red.

El modelo OSI abarca una serie de eventos importantes que se producen durante la comunicación entre sistemas. Proporciona las normas básicas para una serie de procesos distintos de conexión en red:

- El modo en que los datos se traducen a un formato apropiado para la arquitectura de red que se está utilizando.
- El modo en que las PC´s u otro dispositivo de red se comunica.
- El modo en que los datos se transmiten entre los distintos dispositivos y la forma en que se resuelve la secuenciación y comprobación de errores.
- El modo en que el direccionamiento lógico de los paquetes pasa a convertirse en el direccionamiento físico que proporciona la red.

Este modelo, entonces ofrece los mecanismos y reglas que permiten resolver todas las cuestiones anteriores. Cabe mencionar que este modelo es importante precisamente por ser un marco de referencia, de esta forma todos los libros y artículos que hablan sobre la conexión de red lo pueden tomar como referencia Para el estudio de otros modelos es recomendable aprender las funciones de éste y después relacionarlo, de esta forma será fácil aprender otros modelos ligando ideas.

Capa de aplicación
La capa de aplicación proporciona la interfaz y servicios que soportan las aplicaciones de usuario, en otras palabras ésta capa suministra las herramientas que el usuario ve, de una forma tangible interactúan con el usuario.
La capa de uso del modelo de OSI es responsable de proporcionar servicios del usuario final, tales como transferencias de archivo, mensajería electrónica, E-mail, el acceso terminal virtual, y la dirección de la red. Ésta es la capa con la cual el usuario obra recíprocamente.

Capa de presentación
Se encarga de que cada máquina pueda leer e interpretar la información, es decir traduce la información y la convierte a un formato genérico, codifica la información. Otras funciones son la de comprimir los datos y cifrarlos. De esta forma las máquinas hablarán el “mismo idioma”. La capa de presentación del modelo de OSI es responsable de definir la sintaxis que dos anfitriones de la red utilizan comunicar. El cifrado y la compresión deben ser funciones de la capa de presentación.

Capa de Sesión
La capa de sesión es la encargada de establecer el enlace de comunicación o sesión entre las computadoras emisora y receptora, estableciendo la sesión entre ambos nodos (inicia, regula y administra).
La capa de sesión del modelo de OSI es responsable de establecer comunicaciones de proceso a proceso entre los anfitriones que están interconectados en la misma red.

Capa de Transporte
La capa de transporte es la encargada de controlar el flujo de datos entre los nodos que establecen una comunicación, establece el transporte confiable entre dos puntos, sin errores.
La capa de transporte del modelo de OSI es responsable de entregar mensajes entre los anfitriones de una red. La capa de transporte debe ser responsable de la fragmentación y del nuevo ensamble.

Capa de red
La capa de red encamina los paquetes además de ocuparse de entregarlos. Para esto se encarga del direccionamiento lógico y enrutamiento.
La capa de red del modelo de OSI es responsable de establecer las trayectorias para la transferencia de datos a través de la red.

Capa de enlace de datos
Asegura el transporte confiable entre sistemas que comparten un medio de transmisión, es decir, se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor por medio de direcciones físicas llamadas MAC, que se encuentran codificadas en la NIC.
La capa de transmisión de datos del modelo de OSI es responsable de las comunicaciones entre los nodos de red adyacentes.

Capa física
En la capa física las tramas procedentes de la capa de enlace de datos se convierten en una secuencia única de bits que puede transmitirse por el entorno físico de la red.

Cada capa confía en que las demás harán su trabajo, una capa no se interesa por el funcionamiento de las demás, lo único que es de interés es la forma en cómo los datos serán pasados hacia arriba o hacia abajo.

La forma de lograr esto es empacando y desempacando información en los mensajes que se van a enviar, por medio de encabezados que diferencian el contenido de cada capa, como se puede observar en la siguiente figura.

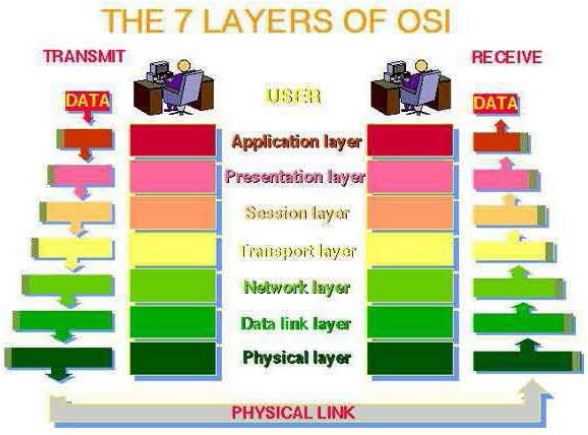


Figura 13. Modelo de Referencia OSI

III.5 Interfaces aéreas. Capa física

El nivel físico (o capa física) recibe una trama binaria que debe convertir a una señal eléctrica, electromagnética, óptica u otra dependiendo del medio de transmisión, de tal forma que a pesar de la degradación que la señal sufra en el medio pueda ser interpretada correctamente en el receptor.

La capa física es la interfaz entre el control de acceso al medio (MAC) y el medio inalámbrico donde los *frames* se transmiten y reciben, esta capa física realiza tres funciones principales:

- Provee de una interfaz para intercambiar *frames* con la capa superior (MAC) para la transmisión y recepción de datos.
- Utiliza una señal portadora y modulación de espectro disperso para transmitir *frame*s utilizados por el medio.
- Provee un indicador de detección de la portadora de regreso al MAC para verificar la actividad en el medio.

Existe un documento que especifica estándares para la capa física (PHY) y la de acceso al medio (MAC), el cual se creo en la Organización Internacional de Estandarización (ISO) y que pertenece al estándar 802.11. En este apartado describen las especificaciones, por lo que en la parte 11 del estándar se proveen tres opciones diferentes de PHY y que cualquier dispositivo tendrá que cumplir si es que quiere tener intercomunicación con equipos de otras compañías.

Propagación

El modelado del canal de radio ha sido históricamente una de las partes más difíciles del diseño del canal de radio y se ha hecho típicamente en forma estadística, basado en medidas tomadas específicamente para sistemas de comunicación propuestos o asignación del espectro.

Tiene como fundamento predecir la intensidad promedio de la señal a una distancia dada del transmisor, para así medir la variabilidad de la intensidad de la señal en las proximidades de localidades particulares.

Ya que existe una necesidad de ser capaces de modelar las pérdidas por trayectoria (estos son modelos de propagación a gran escala: T-R están en el orden de 1000m) y la propagación multitrayectoria (los cuales son modelos de propagación a pequeña escala: T y R están en el orden de unas pocas ondas).

Sabemos que el fenómeno de propagación radio móvil cuenta con muchas variables y es difícil obtener una generalización porque actúan entre otros fenómenos:

- Reflexión
- Difracción
- Dispersión
- Fluctuaciones o desvanecimientos (fading)
- Velocidad del usuario móvil
- Longitud de onda (frecuencia)

Para comprender algunos de los modelos de propagación la estrategia será comenzar por el planteamiento de un modelo sencillo y ajustarlo a las necesidades que se tengan en el modelado.

- Propagación del Espacio LIBRE (antena OMNI-Direccional)

Tomando en cuenta que la densidad de potencia recibida a una cierta distancia d, si la antena radía onmidireccionalmente, será la siguiente

La densidad de potencia recibida a una cierta distancia d:

La potencia recibida PR será igual a:

$$P_R = \frac{P_T}{4\Pi d^2} A_R \eta_R$$

La eficiencia de la antena (η_R), si la antena es buena es de entre .85 a .95

La mayoría de las antenas tienen ganancia sobre un radiador isotrópico:

$$P_R = \frac{G_T P_T}{4\pi d^2} A_R \eta_R$$

El factor GT:

Proporcional al área de radiación efectiva A_T de la antena transmisora

A mayor tamaño de la antena en términos de longitudes de onda, será más estrecho el haz transmitido y será mayor la concentración de energía, la relación ganancia – área está dada por:

$$G_T = \frac{4\pi \eta_T A_T}{\lambda^2}$$

Factor de eficiencia de la antena transmisora

El factor AR se sustituye por el factor GR, el cual obedece a una relación similar:

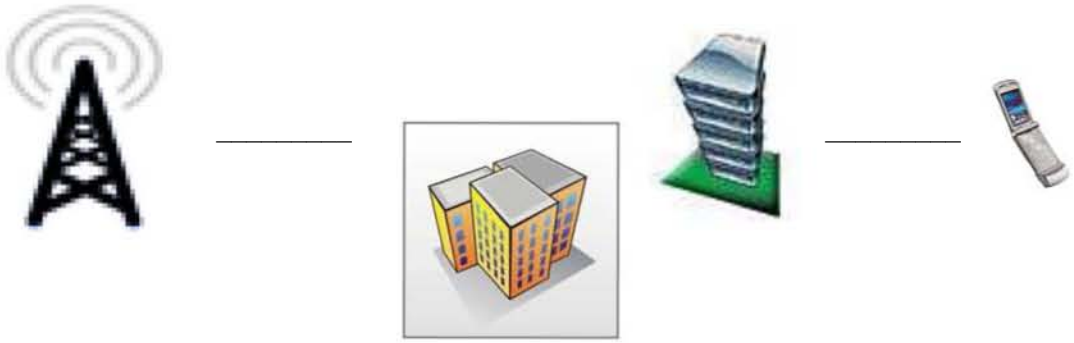
Finalmente:

$$P_R = G_T G_R P_T \left(\frac{\lambda}{4\pi d}\right)^2$$

Esta expresión se utiliza para determinar los requerimientos de potencia para las comunicaciones satelitales, por el tipo de antenas que se manejan.

La propagación en un ambiente celular varía significativamente a este modelo, ya que la antena no tendrá una ganancia tan alta y habrá muchos obstáculos en la línea de vista de la antena transmisora.

Figura 14. Obstáculos en la línea de vista de la antena transmisora



La potencia media medida en el campo lejano (Far Field, es decir distancias de varias longitudes de onda), ya no es n=2, en la mayoría de los casos se tendrá n=3 o n=4.

Los diseñadores de sistemas utilizan un trazado de rayos para determinar el nivel de potencia esperado para una transmisión en interiores.

Hay programas disponibles que computan la potencia y el retardo por dispersión, la mejor aproximación es cuando se usan cuatro rayos:

- Rayo directo
- Rayo reflejado por la tierra
- Dos rayos reflejados por paredes

Algunas veces se usa para posicionar puntos de acceso en redes inalámbricas (mayormente en ambientes interiores)

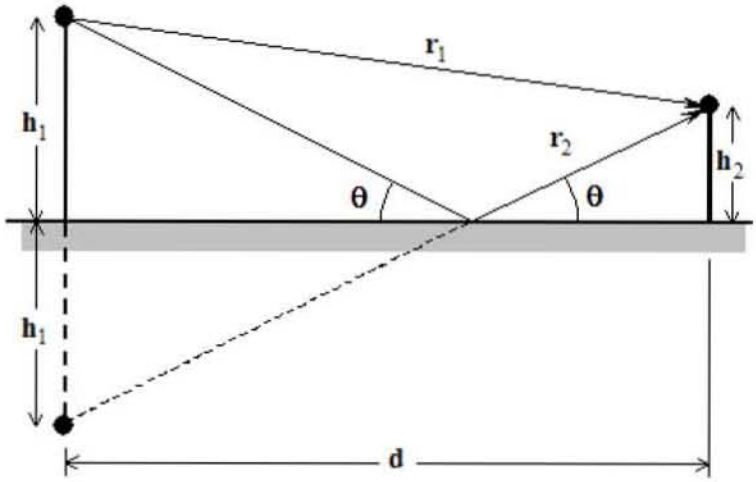


Figura 15. Ejemplo de trazado re rayos para determinar el nivel de potencia

Fluctuaciones Lentas

La potencia recibida medida en el campo lejano varía aleatoriamente alrededor de la potencia promedio.

Una buena aproximación es asumir que la potencia medida en decibeles sigue una transmisión gaussiana o normal, centrada en su valor promedio con desviación estándar que varía entre los 6 a 10 dB

A esta distribución de probabilidad de potencia se le denomina distribución log-normal. A este fenómeno se le conoce como shadow fading

Fluctuaciones Rápidas

Entre más pequeñas sean las distancias en términos de longitudes de onda, habrá mayor variación de la señal. Con moverse el receptor distancias del orden de λ/2 la seña varía algunos dBs.

La señal de radio puede verse severamente distorsionada en el receptor.

Las pequeñas variaciones de la señal recibida se deben a interferencias constructivas y destructivas con otras señales (fluctuaciones por múltiples ondas), estas fluctuaciones siguen dos tipos de distribuciones:

- Rayleigh: para células grandes
- Ricen: para células pequeñas

Rayleigh

La dispersión de Rayleigh (en honor a Lord Rayleigh) es la dispersión de la luz o cualquier otra radiación electromagnética por partículas mucho menores que la longitud de onda de los fotones dispersados. Ocurre cuando la luz viaja por sólidos y líquidos transparentes, pero se ve con mayor frecuencia en los gases. La dispersión de Rayleigh de la luz solar en la atmosfera es la principal razón de que el cielo sea azul. Si el tamaño de las partículas es mayor que la longitud de onda, la luz no se separa y todas las longitudes de onda son dispersadas, como cuando al atravesar una nube, esta se ve blanca, lo mismo pasa cuando atraviesa los granos de sal y de azúcar. Para que la luz sea dispersada, el tamaño de las partículas debe ser similar o mayor que la longitud de onda.

El grado de dispersión de Rayleigh que sufre un rayo de luz depende del tamaño de las partículas y de la longitud de onda de la luz, en concreto, el coeficiente de dispersión y por lo tanto la intensidad de la luz dispersada depende inversamente de la cuarta potencia de la longitud de onda, relación conocida como Ley de Rayleigh. La dispersión de luz por partículas mayores a un décimo de la longitud de onda se explica con la teoría de Mie, que es una explicación más general de la difusión de radiación electromagnética.

La intensidad I de la luz dispersada por una pequeña partícula en un haz de luz de longitud de onda λ e intensidad I_0 viene dada por:

$$I = I_0 \frac{(1+\cos^2\theta)}{2R^2} \left(\frac{2\pi}{\lambda}\right)^4 \left(\frac{n^2-1}{n^2+2}\right)^2 \left(\frac{d}{2}\right)^6$$

Dónde R es la distancia a la partícula, θ es el ángulo de dispersión, n es el índice de refracción de la partícula y d es el diámetro de la partícula.

La distribución angular de la dispersión de Rayleigh, que viene dada por la fórmula $(1+\cos^2\theta)$, es simétrica en el plano perpendicular a la dirección de la luz incidente, por tanto la luz dispersada iguala a la luz incidente. Integrando el area de la esfera que rodea una partícula obtenemos la sección transversal de la dispersión de Rayleigh, σ_s:

$$\sigma_s = \frac{2\pi^5}{3}\frac{d^6}{\lambda^4}\left(\frac{n^2-1}{n^2+2}\right)^2$$

El coeficiente de dispersión de Rayleigh para un grupo de partículas es el número de partículas por unidad de volumen *N* veces la sección transversal. Como en todos los efectos de onda, en la dispersión incoherente las potencias son sumadas aritméticamente, mientras que en la dispersión coherente -como sucede cuando las partículas están muy cerca unas de otras- los campos son sumados aritméticamente y la suma debe ser elevada al cuadrado, para obtener la potencia final.

La fuerte dependencia de la dispersión con la longitud de onda ($\sim\lambda^{-4}$) supone que en la atmosfera la luz azul se dispersa mucho más que la luz roja.En la atmosfera, esto provoca que los fotones de luz azul se dispersen mucho más que los de longitudes de onda mayores a 490nm, por este motivo vemos el cielo azulado en todas direcciones y sólo lo vemos enrojecido cuando miramos hacia el Sol. Cabe destacar que, a pesar del uso del término fotón, la ley de dispersión de Rayleigh fue desarrollada antes de la invención de la mecánica cuántica y por lo tanto, no se basa fundamentalmente en la teoría moderna sobre la interacción de la luz con la materia. No obstante, la dispersión de Rayleig es una buena aproximación a la forma en que la luz es dispersada por partículas mucho más pequeñas que su longitud de onda.

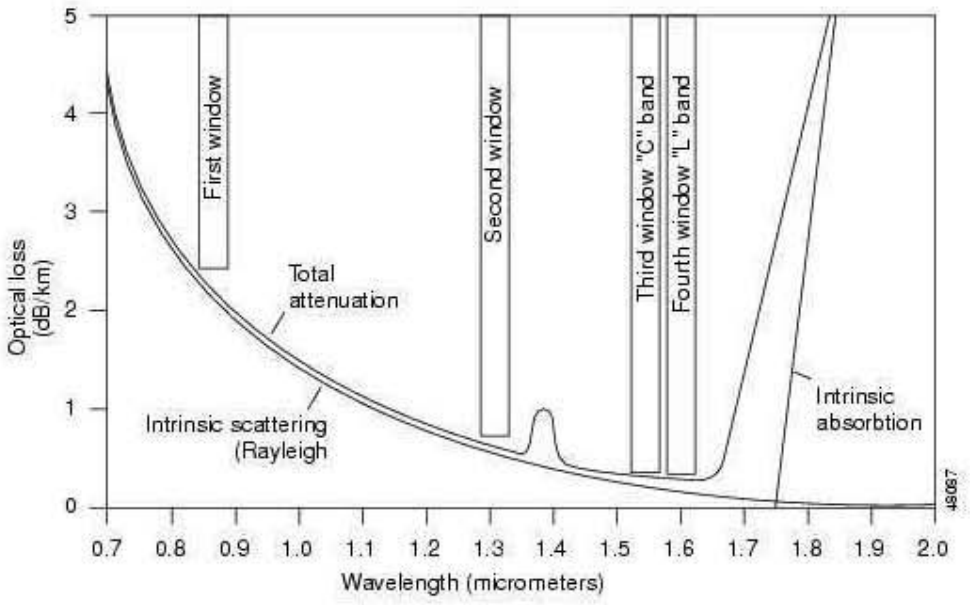


Figura 16. Ventanas de Transmisión

Espectro Disperso

Spread Spectrum (“espectro disperso”) es una técnica de comunicación que por los altos costes que acarrea, se aplicó casi exclusivamente para objetivos militares, hasta comienzos de los años noventa. Sin embargo, comienza a surgir lentamente un mercado comercial, hasta que en nuestros días es común encontrar aplicaciones de este tipo.

La meta de la técnica de espectro disperso es utilizar todo el ancho de banda que se tiene para transmitir, de modo que se reduzca el efecto de interferencia en el medio.

Esta técnica *dispersa* el ancho de banda transmitido de la señal resultante, reduciendo la potencia máxima, pero manteniendo la potencia total en un mismo nivel.

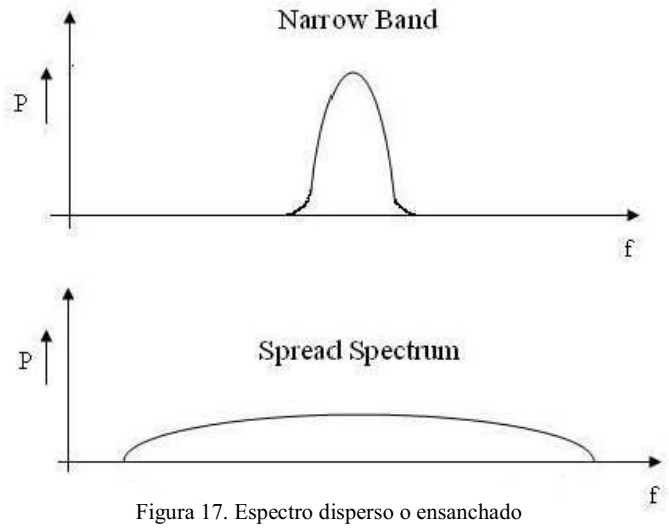


Figura 17. Espectro disperso o ensanchado

FHSS (Frecuency Hopped Spread Spectrum)

Es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia síncronamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

1. Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.
2. Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.
3. Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

Las técnicas que utilizan salto en frecuencia dependen de la diversidad de frecuencias para combatir la interferencia. Básicamente la señal salta de frecuencia en frecuencia siguiendo un patrón dado por un código que dispersa la potencia de la señal sobre un ancho de banda dado.

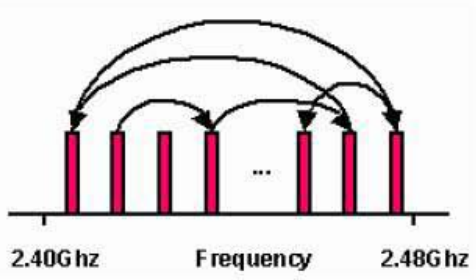


Figura 18. FHSS Frecuency Hopped Spread Spectrum

El transmisor FHSS es un sintetizador de frecuencia de pseudo-ruido controlado por código. La frecuencia de salida instantánea del transmisor salta de un valor a otro basado en una entrada pseudo-aleatoria del generador de códigos. Al variar la frecuencia instantánea se tiene un espectro de salida disperso sobre el rango de frecuencias generado.

El salto de frecuencias en el estándar 802.11 es realizado con modulación de frecuencia gaussiana GFSK. Se utiliza 1 Mbps con GFSK de dos niveles y se utilizan 2 Mbps con una modulación de 4 niveles. Existen ciertas variaciones de acuerdo al lugar donde se opere: Europa y América permiten saltos en el rango de 2402 a 2480 MHz con un espaciamiento de canal de 1 MHz y Japón permite saltos en el rango de los 2402 a 2478 MHz.

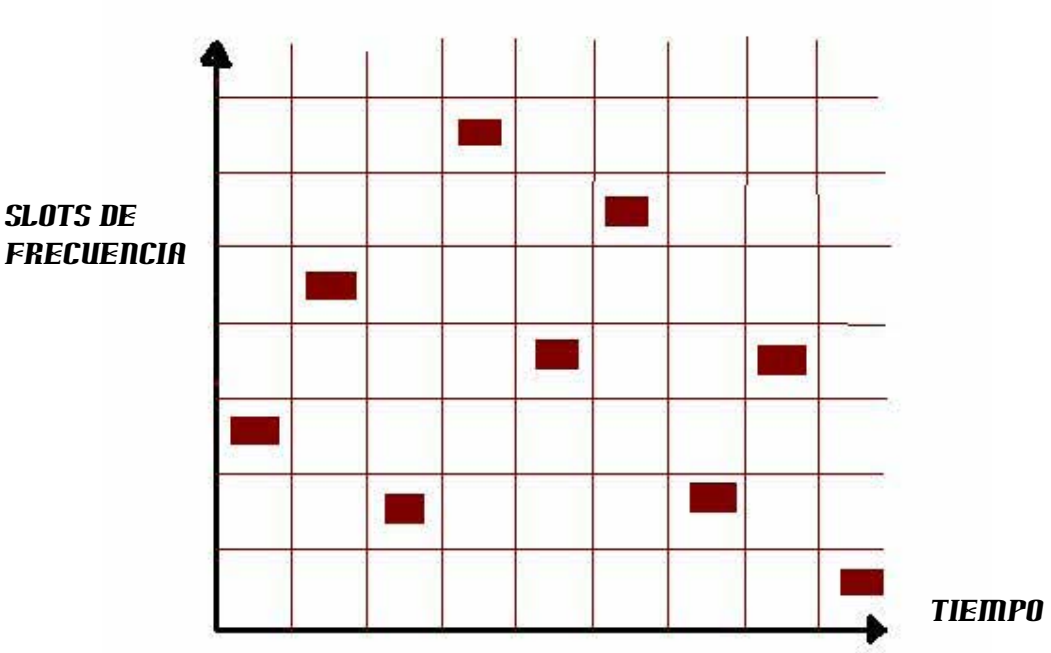


Figura 19. Salto en Frecuencia.
Transmisión de los datos en un determinado Slot de Frecuencia.
Podemos observar cómo varían de forma pseudo-aleatoria en el tiempo

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

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer. Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en le tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica también utiliza la zona de los 2.4GHz, la cual organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltas de 2.5 por segundo.

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps.

En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps. La técnica FHSS sería equivalente a una multiplexación en frecuencia.

DSSS (Direct Sequency Spread Spectrum)

El espectro ensanchado por secuencia directa (D*irect Sequence Spread Spectrum* o *DSSS*), también conocido en comunicaciones móviles como DS-CDMA (Acceso Múltiple por División de Código en Secuencia Directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan. Tanto DSSS como FHSS están definidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN.

El espectro ensanchado por secuencia directa es una técnica de modulación que utiliza un código de pseudorruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido menos al que va dirigida la señal, ya que conocerá el patrón con el que son transmitidos los datos.

Figura 19. Salto en Frecuencia.
Transmisión de los datos en un determinado Slot de Frecuencia.
Podemos observar cómo varían de forma pseudo-aleatoria en el tiempo.

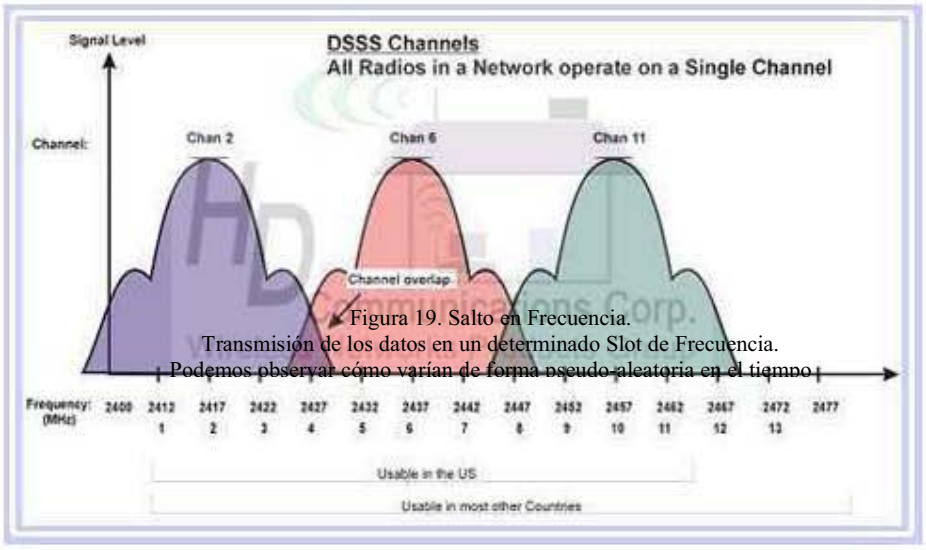
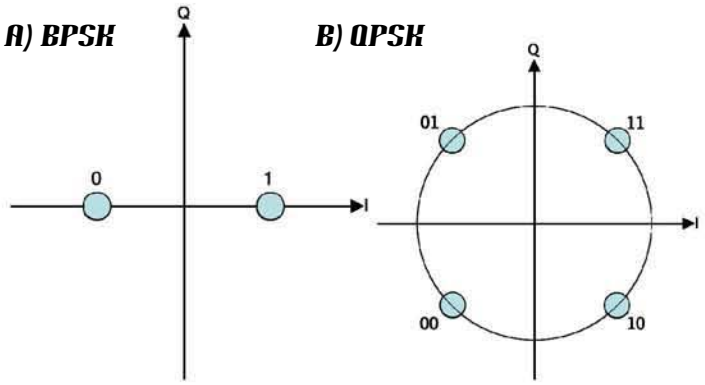


Figura 20. Canales de DSSS en Estados Unidos
Imagen facilitada de HD Communications Corp. para fines sin lucro, que muestra tres de los canales de DSSS utilizados en los EU y en la mayoría de otros países, en donde se puede ver cada espectro ensanchado.

El espectro disperso por secuencia directa utiliza un código de alta velocidad y modulación BPSK para modular a la portadora y realizar la dispersión. Se combinan estas características con tasas de transmisión de datos más pequeñas que también modulan a la portadora ya sea con BPSK o DQPSK (cuadrática diferencial). El código de alta velocidad es un código Baker de 11 bits que tiene buenas propiedades de auto correlación y le da a la forma de onda protección contra interferencia y multitrayectoria.



a) Diagrama de constelación para BPSK (Binary Phase-shift keying)
b) Diagrama de constelación paraQPSK (Quadrature Phase-shift keying)

Figura 21. BPSK & QPSK

Cabe mencionar que en el estándar IEEE 802.11, la técnica de Secuencia directa a diferencia de las técnicas CDMA, sólo utiliza una señal de dispersión predefinida. El receptor común puede operar con una tasa de señal a ruido de 0 dB en el ancho de banda disperso y por lo tanto puede tolerar problemas de multitrayectoria mayores. Algunas de las características de Secuencia Directa en el estándar 802.11 son:

- Tasas de transmisión de 1 y 2 Mbps (modulación DBPSK y DQPSK respectivamente)
- Tasa de símbolos de 1Mbps
- Tasa de chipping de 11 Mbps con una secuencia Baker de 11 chips
- De 3 a 4 canales en la banda de 2.4 a 2.4835 GHz
- 10 dB en ganancia de procesamiento para una modulación eficiente en potencia y desempeño robusto contra interferencia y ruido (10 dB de supresión)
- Protección contra dispersión por retardo de tiempo

Los canales de 802.11b que proveen una transmisión de 11 Mbps en la banda de 2.4 GHz se muestran en la siguiente figura:

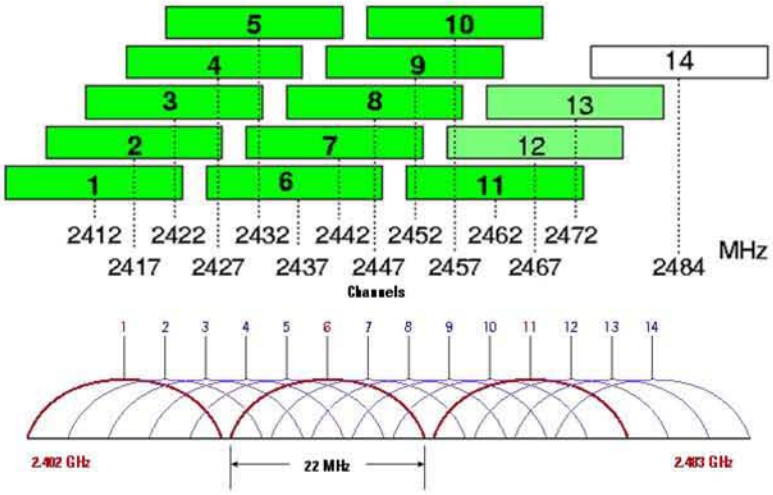


Figura 22. Canales de 802.11 b con transmisiones de 11 Mbps en la banda de 2.4 GHz

En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

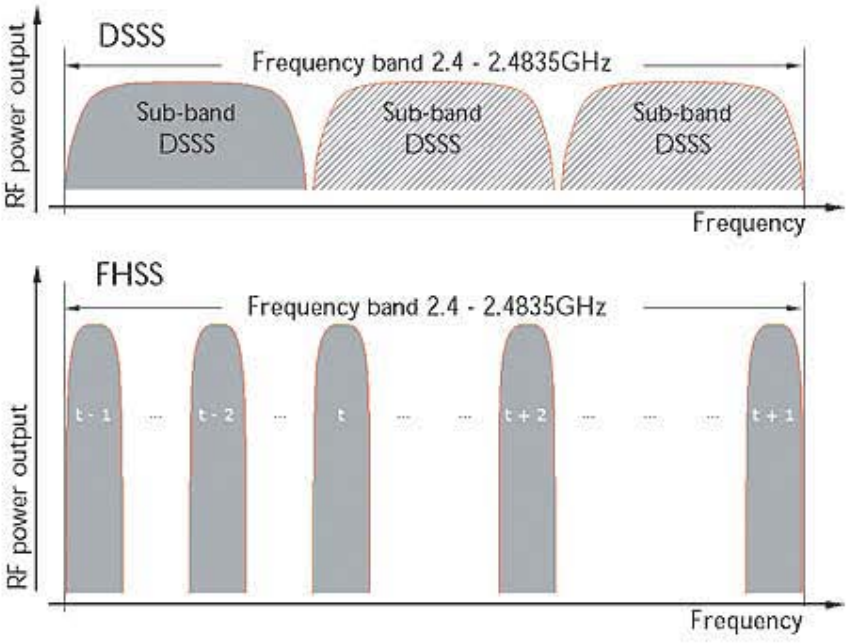


Figura 23. DSSS vs FHSS

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o PseudoNoise). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente:

+1 -1 +1 +1 -1 +1 +1 +1 -1 -1 -1 -1

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10.4 dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación DBPSK *(Differential Binary Phase Shift Keying*) y la modulación DQPSK (*Differential Quadrature Phase Shift Keying*), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

Recientemente el IEEE ha revisado este estándar, y en esta revisión, conocida como 802.11b, además de otras mejoras en seguridad, aumenta esta velocidad hasta los 11Mbps, lo que incrementa notablemente el rendimiento de este tipo de redes.

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país está autorizado a utilizar un subconjunto de estos canales. En el caso de España se utilizan los canales entre 1 y 11, preferentemente los canales 1,6 y 11 para evitar interferencias. En conexiones domésticas, teóricamente, sólo se puede utilizar el canal 6.

En configuraciones donde existan más de una celda, éstas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal.

La técnica de DSSS podría compararse con una multiplexación en frecuencia.

OFDM (Orthogonal Frequency Division Multiplexing)

La modulación por división ortogonal de frecuencia, en inglés *Orthogonal Frequency Division Multiplexing (OFDM)*, también llamada modulación por multitono discreto, en inglés *Discreet Multitone Modulation (DMT)*, es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferente frecuencia.

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, del inglés *Coded OFDM*.

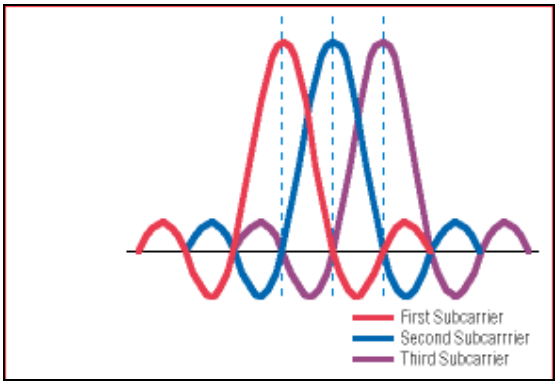


Figura 24. OFDM I

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras *equiespaciadas* que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la IDFT y la DFT respectivamente.

La modulación OFDM es muy robusta frente al multitrayecto, que es muy habitual en los canales de radiodifusión, frente a los desvanecimientos selectivos en frecuencia y frente a las interferencias de RF.
Debido a las características de esta modulación, las distintas señales con distintos retardos y amplitudes que llegan al receptor contribuyen positivamente a la recepción, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

Entre los sistemas que usan la modulación OFDM destacan:

- La televisión digital terrestre DVB-T, también conocida como TDT.
- La radio digital DAB.
- La radio digital de baja frecuencia DRM.
- El protocolo de enlace ADSL.
- **El protocolo de red de área local IEEE 802.11a/g, también conocido como Wireless LAN.**
- El sistema de transmisión inalámbrica de datos WiMAX

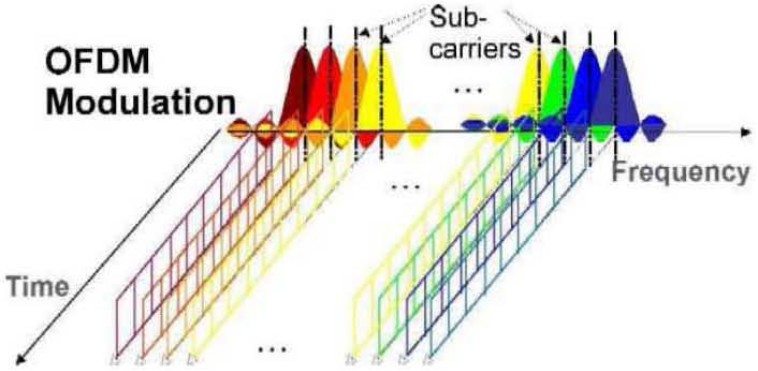


Figura 25. OFDM II

Formato del Frame en la capa PHY

La capa física se encuentra dividida en dos subcapas: PDM (*Physical Medium Dependent*) y PLCP (*Physical Layer Convergent Protocol*): la primera tiene la función de definir las características de transmisión y recepción en el medio inalámbrico; la capa PLCP es llamada así por utilizar dicho protocolo, el cual se encarga de establecer una comunicación entre las capas PDM y MAC. Esta subcapa puede emplear dos formatos de trama (con preámbulo largo y corto), desarrollado posteriormente para mejorar el rendimiento de red.

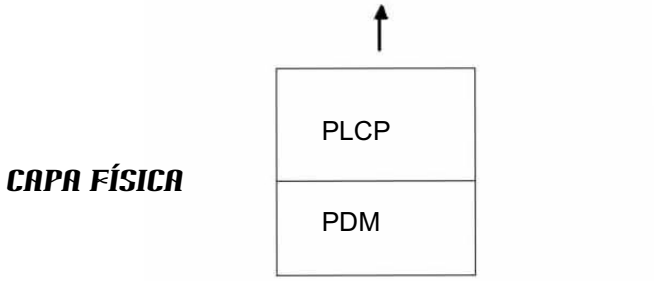


Figura 26. División de la capa física PHY en dos subcapas

El preámbulo PLCP consiste en dos campos, uno de sincronización de la señal de 128 bits para preámbulo largo y 56 bits para preámbulo corto y el delimitador de inicio de trama. Ambos son transmitidos a 1 Mbps con DBPSK.

El encabezado PLCP, contiene 48 bits de información y consta de 4 campos:

- **Señal** – Indica qué tan rápido serán transmitidos los datos contenidos en el PSDU (PLCP Data Unit)
- **Servicio** – Indica la modulación empleada para el PSDU

- **Longitud** – Indica la longitud del campo PSDU
- **CRC (Cyclic Redundancy Check)** – Valor calculado de acuerdo con la información de los cuatro campos d el encabezado para detección de errores.

Figura 27. Frame de la Capa Física

El contenido del encabezado es el mismo para el preámbulo largo y corto, sin embargo para el primero la información es transmitida a 1Mbps con DBPSK y para el segundo a 2 Mbps con DQPSK. Los datos contenidos en el PSDU pueden ser transmitidos con velocidades de 2, 5.5 y 11 Mbps para el preámbulo corto y 1, 2, 5.5 y 11 Mbps para preámbulo largo. La trama completa compuesta del preámbulo PLCP, encabezado y PSDU es denominada PPDU (PLCP Protocol Data Unit).

Comparación entre modalidades PHY

Tabla 4. Comparativa que resume las características de las modalidades del estándar 802.11

ESTÁNDAR	802.11a	802.11b	802.11g
Frecuencia	5 GHz	2.4 GHz una banda muy utilizada por lo que hay interferencia con otros dispositivos que utilicen la misma banda.	2.4 GHz una banda muy utilizada por lo que hay interferencia con otros dispositivos que utilicen la misma banda.
Velocidad teórica	54 Mbps	11 Mbps	54 Mbps
Throughput promedio	27 Mbps	4 – 5 Mbps	20 – 25 Mbps
No. De canales/ utilizables	12 / 8	11 / 3	11 / 3
Rango*	Rango menor que en 802.11 b y g, debido a su frecuencia de operación tan alta.	Rango alto, puede trabajar entre pisos y paredes	Rango alto, puede trabajar entre pisos y paredes
Compatibilidad	Incompatible con 802.11 b y g	Ampliamente adoptado, compatibilidad con 802.11g	Muy compatible
Popularidad	Poco uso	Muy extendido	Entrando al mercado
Costo	Caro	Bajo	Regular y disminuyendo

*El rango dependerá de la ganancia de la antena, potencia de transmisión, sensibilidad de recepción del radio y obstáculos entre origen y destino, además de la velocidad de movimiento.

III.6 Acceso al medio

En los protocolos IEEE 802 para redes LAN compartidas de acceso múltiple, la capa de enlace (*data link*) está dividida en dos subcapas: la capa superior LLC *(Logical Link Control*), que provee una forma de direccionar una estación en una LAN e intercambiar información con ella y la capa inferior MAC provee la interfaz entre el LLC y el medio en particular de la red que esté siendo utilizada (Ethernet, Token ring, etc.).

La capa MAC reparte datos agrupados en un *frame* para que se transmitan por la red, y luego pasa este *frame* a la interfaz de capa física donde son transmitidos en forma de bits. La información se envía en distintos frames que se transmiten uno a la vez por la red. Si un frame se corrompe (es decir, que tiene errores) durante la transmisión, solo es necesario reenviar dicho frame y no la información completa.

El otro trabajo de la capa MAC es la de controlar el acceso al medio que es compartido por todos los dispositivos conectados a la red. Si dos estaciones fueran a transmitir al mismo tiempo, los datos se mezclarían y se dañarían por lo que no sería posible la comunicación.

Los métodos de acceso primario son de contención y de detección de la portadora.

Como todo en la vida existen diferentes clasificaciones de las técnicas de acceso al medio, una de ellas es por el método de sincronización. Dependiendo del método de sincronización temporal, los mecanismos de control de acceso al medio (MAC) se pueden clasificar en:

- **Sincrónicos**: existe un tiempo limitado durante el cual un dispositivo puede accesar el medio de comunicación. Una vez cumplido su plazo debe esperar su turno nuevamente. Este tipo de acceso es característico de las redes con topología tipo anillo.
- **Aleatorios:** este tipo de técnica no impone un límite de tiempo, es decir, cuando un dispositivo desea transmitir, lo intenta y si tiene éxito lo continua haciendo hasta que ya no tenga más información que transmitir o no pueda accesar el canal nuevamente. Las redes con topología bus utilizan usualmente este método.

La primera técnica tiene la desventaja del retardo que debe sufrir la información de un nodo que aún no se le ha signado su tiempo de transmisión. Peor es el caso si esta espera se produce cuando los demás nodos no poseen información que transmitir, pero igual se les asigna su tiempo de transmisión, es decir es una transmisión justa para todos los nodos que desean transmitir, aún si se encuentran en estado *idle*.

La segunda técnica presenta la desventaja de las colisiones generadas al haber dos estaciones o más queriendo accesar el canal en forma simultánea.

De estas técnicas de acceso las más difundidas son:
Sincrónicas

- Reservación TDMA (*Time Division Multiple Access*), utilizado en enlances WAN T1/E1 y X.25
- Polling, ampliamente usado en smart terminals en los años 70 y hoy en día en buses de terreno (fieldbus) para sensores inteligentes.
- Token Passing (Permiso de Transmisión o Paso de Testigo), usado en los estándares IEEE802.4, IEEE802.5 y Arcnet.

- WDMA (Wavelength Division Multiple Access), para comunicaciones a través de fibra óptica

Asincrónicas

- ALOHA, desarrollo experimental de los años 70.
- CSMA, perfeccionamiento de ALOHA.
- CSMA/CD, técnica del estándar IEEE802.3 (Ethernet).
- MACAW (Multiple Access with Collision Avoidance), usada en comunicaciones wireless (IEEE802.11).

Protocolos de contención

Aloha

Este método de acceso al medio es el precursor de varias estrategias de acceso aleatorio actuales. En este esquema un usuario que desee transmitir lo hace en cualquier momento, sin ninguna estrategia. A causa de esto es probable que dos o más mensajes se traslapen en el tiempo, causando una colisión. Dicha colisión es detectada por cada estación y cada una de estas intenta retransmitir después de transcurrido un tiempo aleatorio, siguiendo un algoritmo de resolución de colisiones, para evitar una nueva colisión.

Este método es conocido y considerado como el método de acceso aleatorio más básico. Este protocolo fue ideado en los años 70 en la Universidad de Hawaii como una solución al acceso al medio en redes de computadores mediante enlaces radioeléctricos. Desde entonces ha sido uno de los protocolos que más ha influido en el mundo de las redes de computadoras, y muchas han sido las mejoras que le han sido aplicadas. Las estaciones que utilizan este algoritmo transmiten inmediatamente después de tener un paquete listo, sin determinar si el canal está siendo utilizada o no.

Una vez transmitido el paquete le corresponde a la estación transmisora determinar si este alcanzo su destino en forma íntegra, para lo cual la estación remota debe enviar una señal de recepción, los errores en la transmisión de información son detectados al chequear la paridad del paquete transmitido en el extremo receptor.

Una transmisión exitosa es indicada con un reconocimiento positivo. Este reconocimiento normalmente es enviado junto con un paquete de información, para aprovechar al máximo las potencialidades del canal.

Al no llegar un reconocimiento positivo, la estación transmisora asume que el paquete sufrió una colisión y que debe retransmitir la información. Si el paquete es retransmitido inmediatamente y otra estación realiza lo mismo se producirá otra colisión. Para evitar esto, una estación determina cuando retransmitir de acuerdo a un algoritmo llamado *backoff algoritm*. Este algoritmo consiste en seleccionar un número aleatorio y retardar la retransmisión en el tiempo que se demora en transmitir un paquete multiplicado por este número. Si todas las estaciones seleccionan este número en forma independiente, existe una alta probabilidad de que no se produzcan colisiones futuras y caer así en un ciclo infinito de errores.

La limitación del flujo de transmisión máximo de ALOHA simple, puede ser incrementada al doble, implementando un sistema de división de tiempo de transmisión en ranuras y permitiendo la transmisión de información sólo al comienzo

de una ranura. Este mecanismo es conocido como ALOHA ranurado y será visto a continuación.

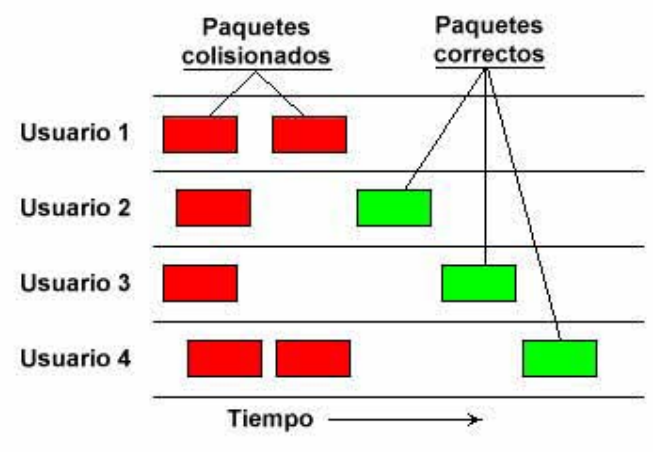


Figura 28. Usuarios que intentan transmitir bajo el protocolo Aloha

En esta figura se puede observar a diferentes estaciones (usuarios) que están transmitiendo en cualquier momento y esto puede causar que algunos paquetes colisionen. La relación entre el tráfico ofrecido, G, y el rendimiento del protocolo viene dada por:

$$\xi = Ge^{-2G}$$

El máximo rendimiento que se obtiene con ALOHA se da cuando G=0.5, y es de 0.18, o sea que cuando se alcanza la mejor utilización del canal, ésta es de un 18%. Por supuesto que no es un resultado muy bueno, pero la sencillez del protocolo hace que sea un protocolo muy atractivo, y susceptible de ser mejorado.

Aloha Ranurado

Un método para mejorar el rendimiento del canal ALOHA es el denominado ALOHA ranurado. En este caso el eje temporal se divide en intervalos discretos que corresponden con un paquete y que se llaman ranuras. Ahora el usuario no puede transmitir sus datos en el momento en que quiera, sino que tiene que esperar hasta el comienzo de una ranura.

La probabilidad de colisión disminuye puesto que ésta sólo se puede producir en el comienzo de un ranuna, y podemos tener la seguridad de que un paquete que se ha empezado a transmitir bien completará la transmisión de manera correcta. En caso de colisión se espera ahora un número aleatorio de ranuras.

La relación entre el tráfico ofrecido y el rendimiento del ALOHA ranurado viene dada ahora por

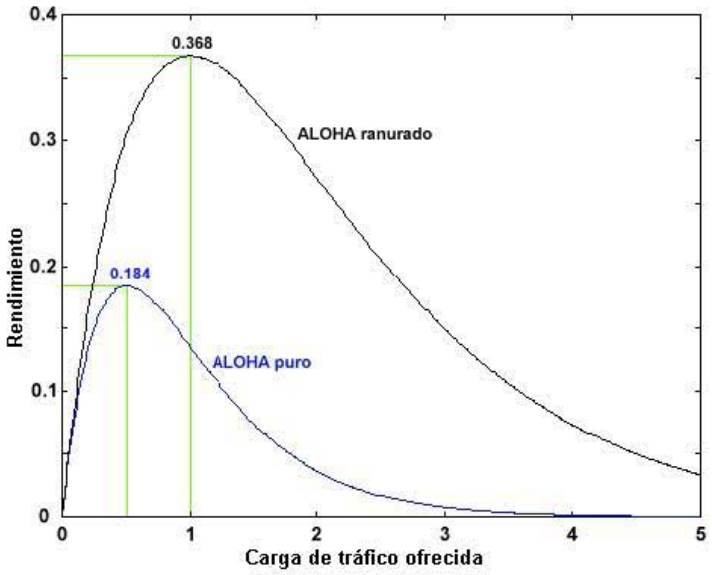
$$\xi = Ge^{-G}$$

Una ranura es normalmente el tiempo de transmisión de un paquete. Este esquema requiere una sincronización de todas las estaciones.

Este algoritmo utiliza hardware especial en cada estación, para detectar el estado del canal de transmisión, determinar si el canal está ocupado y retardar el envío de la información. Esta característica normalmente disminuye las colisiones y mejora el desempeño de la red. Este algoritmo puede operar con o sin ranuras de tiempo.

Al igual que en Aloha, si ocurre una colisión cada estación espera un tiempo aleatorio dado por una distribución exponencial, como puede observarse en la relación, se consigue una significativa mejora del protocolo, teniéndose ahora un rendimiento máximo de 0.36 para G=1, es decir una utilización del canal del 36%.

Figura 29. Rendimiento vs Carga de tráfico ofrecida para Aloha y Aloha Ranurado



Protocolos de Detección de la portadora

CSMA

En este tipo de protocolos la estación que desea transmitir, primero escucha el canal de transmisión para ver si este está libre. Si es así, la estación transmite los datos. En caso contrario la estación no transmite y espera un tiempo aleatorio antes de volver a escuchar el canal.

Aún así, se puede dar el caso en que dos estaciones que quieren transmitir escuchen el canal al mismo tiempo, y al ver que el canal se encuentra libre transmiten sus respectivos datos ocasionando una colisión. También se puede dar el caso que por retardos de propagación una estación detecte erróneamente un canal libre.

Este tipo de esquema reduce en gran manera el número de colisiones, sin embargo es algo ineficiente ya que desperdicia el uso del canal, desperdiciándose tiempos muertos en los que no se realiza ninguna transmisión.

Después de la transmisión de un paquete todas las terminales esperan un tiempo predeterminado de acuerdo al nivel de prioridad de sus paquetes (espaciamientos entre paquetes)

- DCF-IFS (DIFS): Usado para la contención, prioridad más baja, retardo más largo.
- CORTO-IFS (SIFS): Usado para prioridad alta tal como ACK´s, CTS, etc. Tiene la duración de tiempo más baja.
- PCF-IFS (PCF): la tasa tiene segunda prioridad con duración entre DIFS y SIFS.

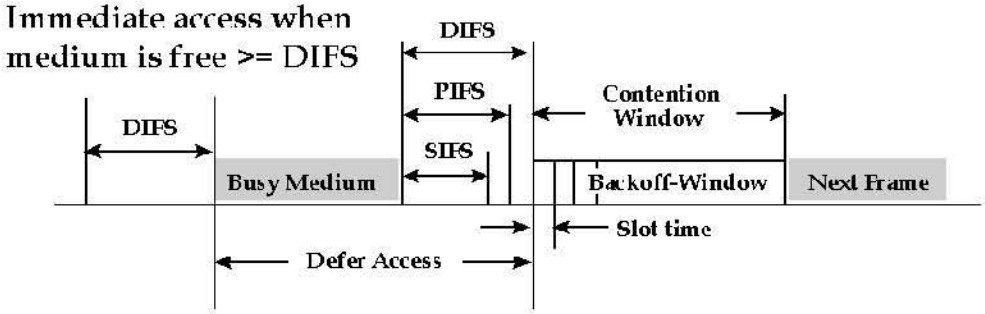


Figura 30. Tiempos para la trasmisión en CSMA

Entonces tenemos que el diagrama de flujo que seguirán lo dispositivos para transmitir será el siguiente:

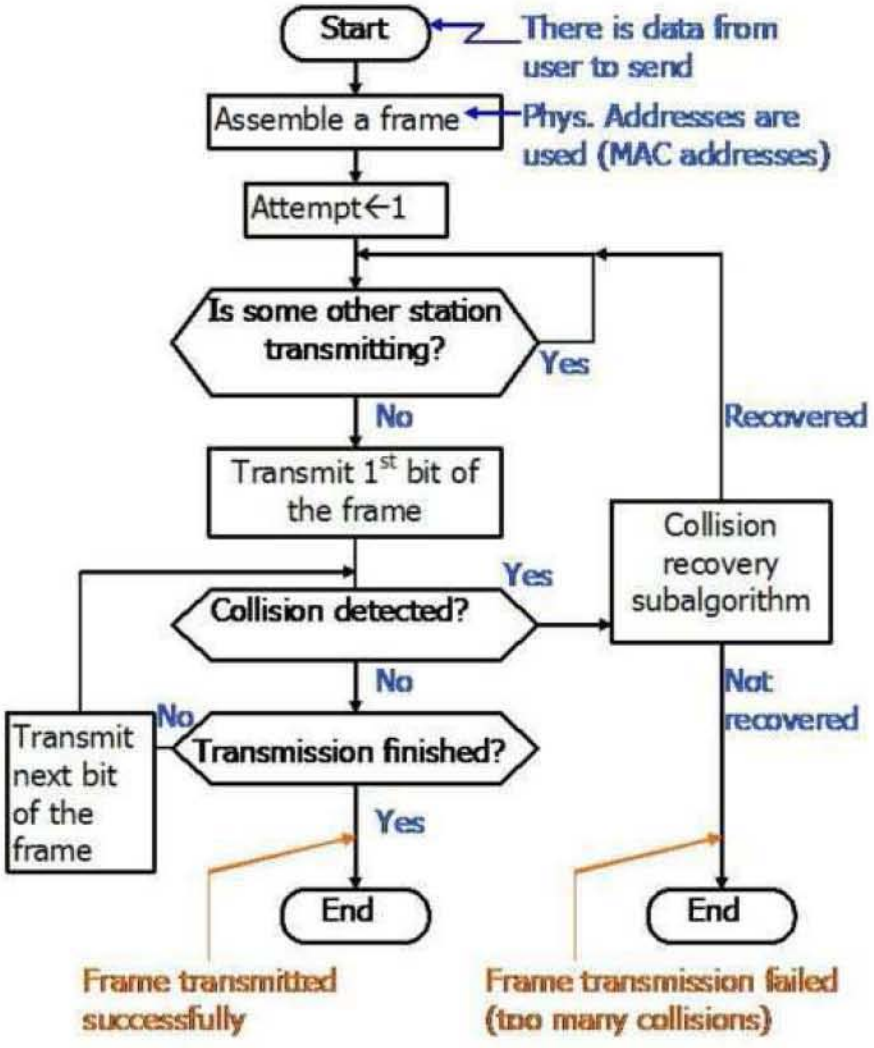


Figura 31. Diagrama de Flujo para transmisión

El Backoff Exponencial que aparece en la penúltima figura tiene como objetivo adaptar los intentos de re-transmisión de acuerdo a la carga estimada de tráfico:

- Carga pesada: esperar mucho
- Carga ligera: esperar poco

De tal manera que su obligación es minimizar la probabilidad de colisión y minimizar el tiempo de espera, para lo cual se basa en lo siguiente:

- Si es primera colisión: escoge K entre {0,1}; el retraso es K x 512 bit [tiempo de transmisión]
- Después de la segunda colisión: escoge K entre {0,1,2,3}
- Después de 10 o más colisiones, escoge K entre {0,1,2,3,4,… 1023}

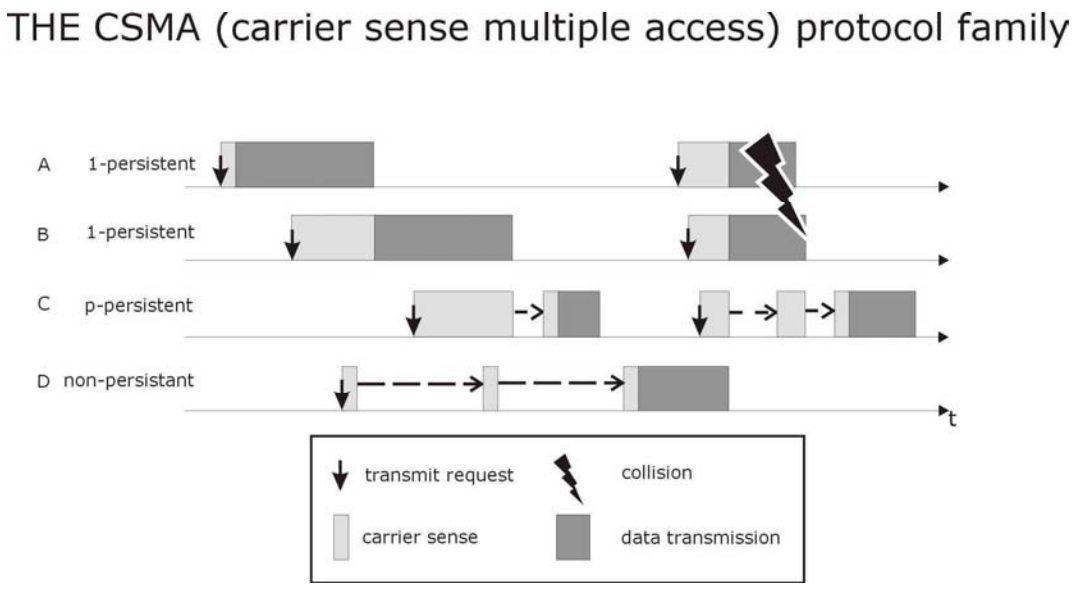


Figura 32. Familia de Protocolos CSMA

Las diferentes técnicas de acceso al medio que hemos visto tienen peculiaridades como la eficiencia y por lo tanto tendrán distintas gráficas de utilización de canal, mostradas en la siguiente figura:

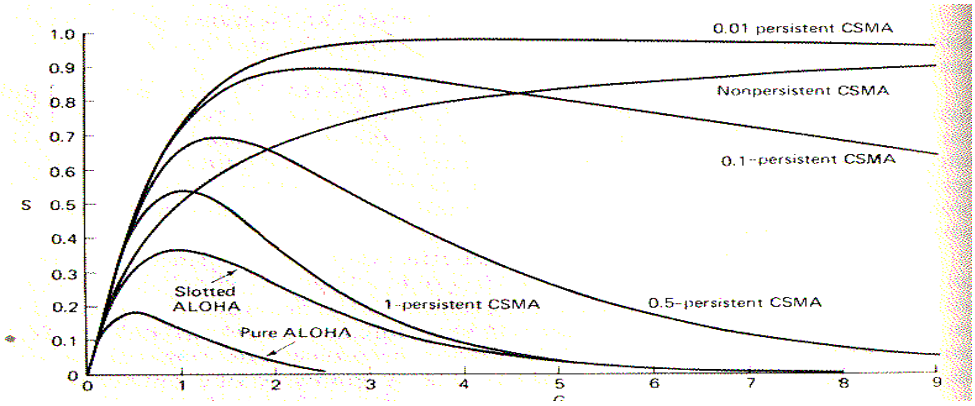


Figura 33. Comparación de la utilización del canal contra carga de varios protocolos de acceso

Terminales Ocultas

Una limitación común de los sistemas LAN inalámbricos es el problema del "nodo oculto". Esto puede romper un 40% o más de las comunicaciones en un ambiente LAN muy cargado. Ocurre cuando hay una estación en un grupo de servicio que no puede detectar la transmisión de otra estación, y así descubrir que el medio está ocupado. El problema del nodo oculto ocurre en redes de punto a multipunto. Este problema puede surgir cuando hay tres o más nodos presentes.

En un caso práctico, se da la siguiente situación:

- La estación A ve a la estación B.
- La estación B ve a la estación A y a la estación C.
- La estación C ve a la estación B.
- La estación A no ve a la estación C.

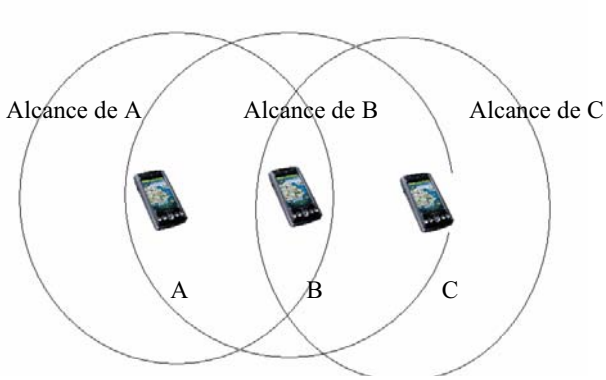


Figura 34. Problema de las Terminales Ocultas

2. Mientras A está transmitiendo, C quiere enviar una trama a B. Detecta el medio libre ya que no capta la emisión de A y transmite.
3. Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas

Solución

Para resolver este problema, la MAC usa un esquema de reservación del canal, es decir, que utiliza el esquema RTS/CTS, por lo que consiste ahora en lo siguiente:

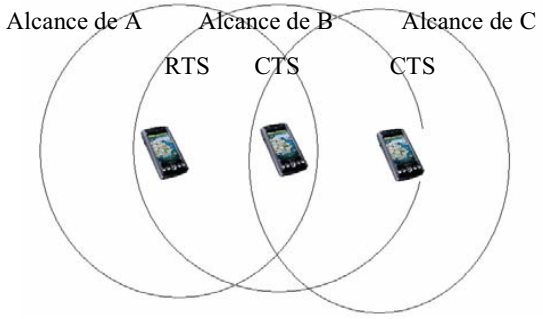


Figura 35. Solución al problema de las Terminales Ocultas

1. Antes de transmitir el frame, A envía un mensaje RTS.

2. B responde al RTS con un CTS.
3. C no capta RTS, pero si el CTS. Sabe que no debe transmitir durante el tiempo equivalente a 500 bytes.
4. A envía su frame de manera segura, evitando colisiones con otras estaciones

A pesar de que el uso de RTS/CTS resuelve el problema de las terminales ocultas y evita las colisiones, también introduce una carga adicional en el protocolo y reduce el rendimiento. Por este motivo el protocolo RTS/CTS sólo se activa cuando los paquetes alcanzan un tamaño determinado.

En algunos sistemas WLAN este tamaño puede determinarlo el administrador (umbral de RTS/CTS). Los porcentajes de errores de bits en las redes inalámbricas son bastante superiores a los de las redes cableadas tradicionales.

Puede que las tramas grandes se acerquen al número de bits en los casos en que la probabilidad de que se produzca un error sea del 100%. Esto implica que todos los bloques podrían fallar incluida la retransmisión.

A fin de reducir esta probabilidad, el transmisor puede fragmentar las tramas grandes y posteriormente, el nodo receptor las puede volver a unir.

A pesar de que esto podría aumentar el tráfico, se reduce la probabilidad de error y en caso de error, también se reduce la retransmisión.

En algunos sistemas WLAN el tamaño del paquete más grande (umbral de fragmentación) puede ser ajustado por el administrador de red.

III.7 Características y funcionamiento de una WLAN

Como he venido manejando, la solución de implementar una WLAN para la transmisión y recepción de datos sin cables es muy factible para los edificios de oficina, campus escolares, o bien en casas particulares es sumamente viable y actualmente muy popular ya que permite que múltiples usuarios accedan a una conexión a Internet y dentro de él obtengan todos los beneficios de los servicios que son proporcionados en línea, llegando a la implantación en la vida real del concepto de sociedad de la información.

Algunos Aeropuertos empiezan (si no es que ya cuentan con la infraestructura) a poner Access Points en las salas de espera, para ofrecer a sus usuarios un servicio de valor agregado, asimismo lo hacen algunos restaurantes y cafeterías para atraer clientes que cuenten con dispositivos apropiados para navegar sin cables al mismo tiempo que consumen sus productos.

Otros nombres para WLAN son 802.11 o WiFi, aunque no están de todo mal, es mejor mencionar cada cosa por su nombre, 802.11 es el estándar y WiFi la tecnología. Existen diferentes versiones de las WLAN´s que se diferencian por la velocidad de transmisión y la frecuencia de operación (por ejemplo 802.11 a maneja una velocidad de 54Mbps a una frecuencia de 5GHz y 802.11b transfiere datos a una velocidad de 11Mbps en la banda de 2.4 GHz), mismas que serán revisadas en subtemas siguientes.

El Canal de radio inalámbrico

WLAN – WiFi Wireless Local Area Network (Red de área local inalámbrica)

Una WLAN es un sistema de comunicaciones transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona *conectividad inalámbrica* dentro de una pequeña área limitada por el alcance del sistema (edificio, área residencial/urbana, oficina o de un campos universitario).

Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) para redes locales inalámbricas.

Como todos los estándares 802 para redes locales del IEEE, en el caso de las WLAN, también se centran en los dos niveles inferiores del modelo OSI, el físico y el de enlace, por lo que es posible correr por encima cualquier protocolo (TCP/IP o cualquier otro) o aplicación, soportando los sistemas operativos de red habituales, lo que supone una gran ventaja para los usuarios que pueden seguir utilizando sus aplicaciones habituales, con independencia del medio empleado, sea por red de cable o por radio.

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro disperso (spread spectrum). En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Comission), la

agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum (SS), con las opciones DS (Direct Sequence) y FH (Frequency Hopping).

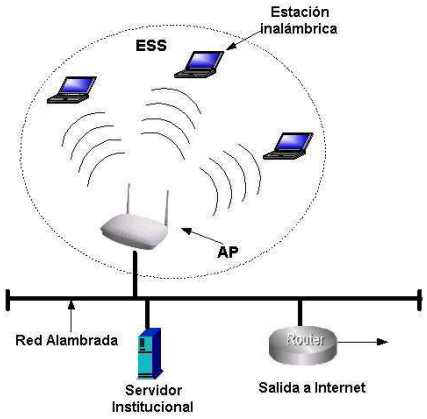


Figura 36. Utilización de una Red Inalámbrica de WiFi típica, con un Access Point y la salida a Internet por medio de la Red alambrada

La técnica de espectro ensanchado es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.

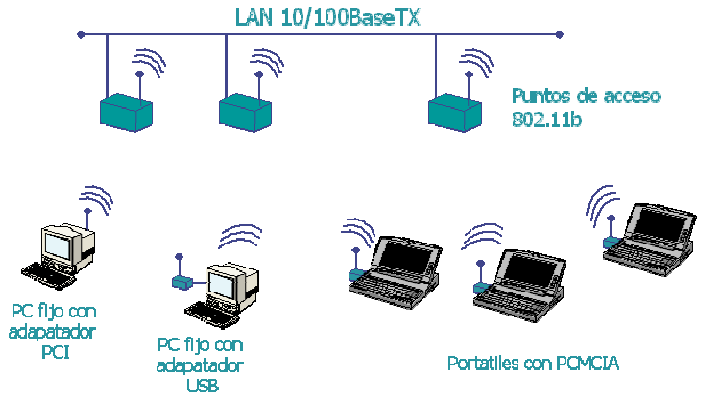


Figura 37. Otra Red Inalámbrica típica, con diferentes elementos que acceden a la Red por medio de tarjetas de distinta naturaleza, pero para un mismo fin

La principal ventaja de este tipo de redes (WLAN), aparte de no necesitar licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.

También, presentan alguna desventaja, o más bien inconveniente, que es el hecho de la "baja" velocidad que alcanzan, por lo que su éxito comercial era escaso hasta 2004.

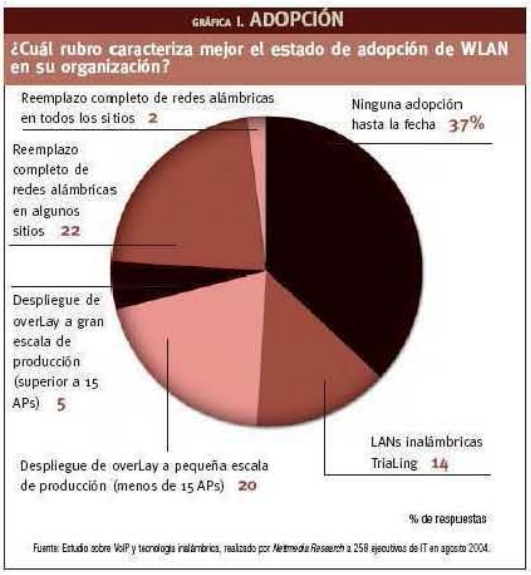


Figura 38. Gráfica que nuestra la preferencia de las WLAN en las organizaciones Fuente: Estudio sobre VoIP y tecnología Inalámbrica realizado por Netmedia Research a 258 ejecutivos de IT en agosto de 2004

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En 1993 también se constituye la IrDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil (mobile computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Por otra parte, WLANA (Wireless LAN Association) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

En junio del año 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbit/s, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia, FHSS en la banda de 2,4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio MAC (Medium Access Control) es mediante escucha pero sin detección de colisión, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Además de las redes inalámbricas (WLAN), el crecimiento de las tecnologías inalámbricas ha ido incrementándose de una forma sumamente grande.

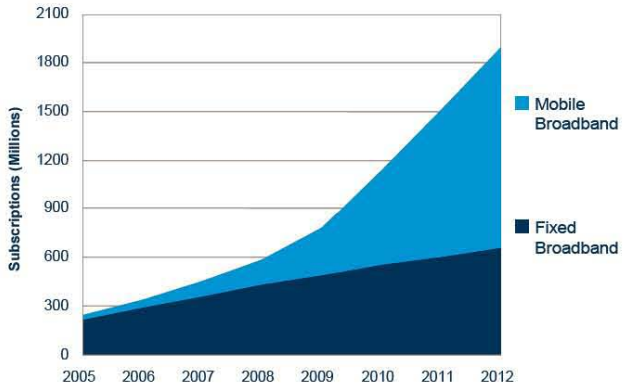


Figura 39. Crecimiento estimado de subscriptores de redes según expectativas de Ericsson para los próximos años

La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es Spread-Spectrum y con acceso por división de código (CDMA), lo que conlleva a que el medio radioeléctrico es compartido, ya sea por secuencia directa DSSS o por saltos de frecuencia en FHSS.

El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implicara que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2,4 GHz está reglamentada como banda de acceso pública y en ella funcionan gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth.

El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una interfaz física.

III.8 Comparativa entre tecnologías

Ahora, recapitulando lo que se ha visto en capítulos anteriores, tenemos distintas clasificaciones de las redes inalámbricas, dos de estas subramas son WMAN (menos a 5 km) y WLAN (menos a 100m), que utilizan tecnologías de diferente naturaleza para transmitir datos.

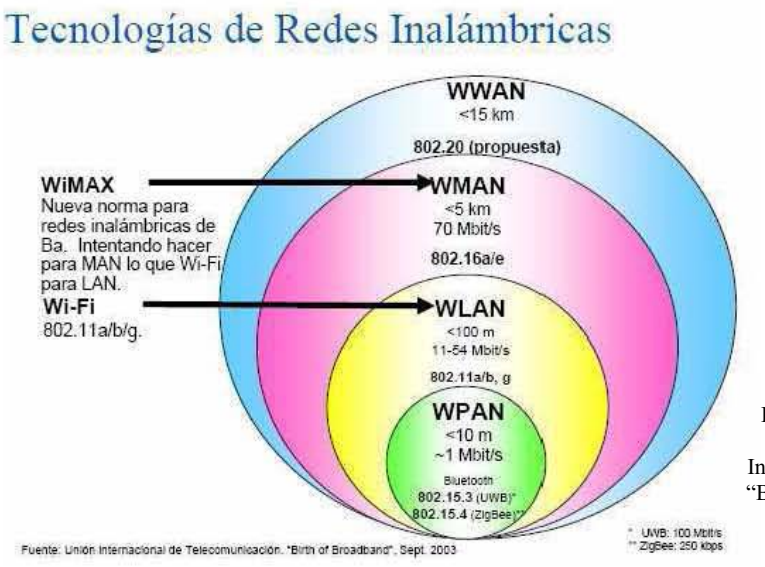


Figura 40. Tecnologías de Redes Inalámbricas. Fuente: Unión Internacional de Telecomunicación. "Birth of Broadband, Septiembre de 2003

¿Las tecnologías WiFi y WiMax son complementarias o están en competencia?

Todos los especialistas tienen su punto de vista para contestar esta respuesta, la mayoría de ellos tienen la propia corriente a la que apoyan. Ambas tecnologías (móvil e inalámbrico) proporcionan acceso inalámbrico a Internet a alta velocidad, pero cada tecnología tiene su nicho de aplicaciones en el mercado. WLAN cubren áreas más pequeñas y tiene movilidad limitada, sin embargo proporcionan altas velocidades de transmisión.

Los sistemas 3G soportan voz, amplia cobertura y alta velocidad, son adecuados para ser desplegados en áreas con demanda moderada o de baja densidad en donde se requiere alta movilidad.

Las aplicaciones de WiFi, entre otras son:

- Acceso a Internet doméstico
- Redes profesionales
- Hotspots. Acceso público
- Conexión de periféricos (impresoras)
- En Europa es utilizado para el acceso a Internet en trenes de alta velocidad y metro.
- Para mejorar la eficiencia de trabajo en entornos hospitalarios, fábricas, oficinas, etc.

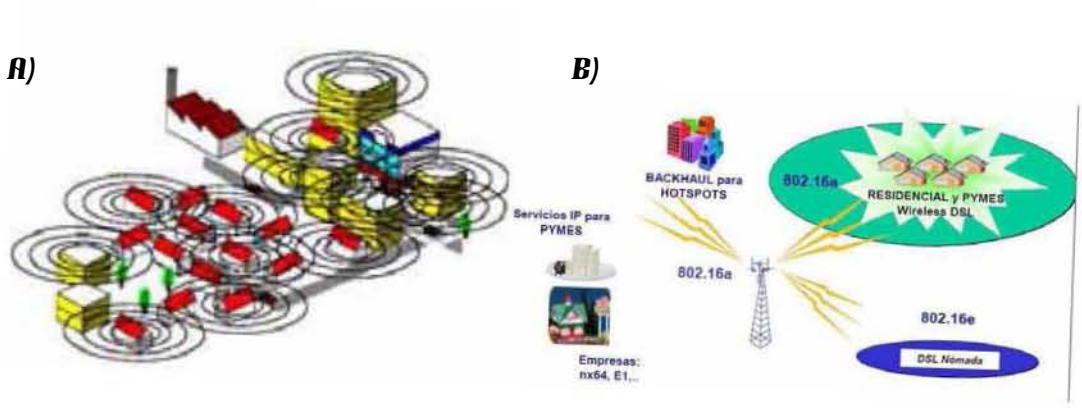


Figura 41. WiFi vs WiMAX
a) Aplicaciones de la Tecnología WiFi
b) Aplicaciones de la Tecnología WiMAX

Por otra parte la tecnología WiMax fue presentada como la opción vanguardista de las redes inalámbricas, teniendo las siguientes características:

- Eficiencia espectral (prometiendo mayor eficiencia y cobertura)
- QoS (Calidad del Servicio, varios niveles adecuados a cada exigencia)
- Seguridad (Autenticación y Encriptación)
- Tarjetas económicas para PC (todavía los precios son mayores que para WiFi)
- Portabilidad y elementos nómadas (plug and play)

Beneficios de WIMAX

- Reducción de Costos y Riesgo de Inversión
  Múltiples fuentes / suministradores con garantía de interoperabilidad
- Escalabilidad de Equipo y capacidad
  Canalizaciones flexibles (Acomoda el uso del espectro disponible, en bandas licenciadas y no licenciadas; Incorporación de nuevos sectores para optimizar la capacidad por celda, permitiendo adaptarse al número de usuarios reales en cada momento; adecuación del protocolo MAC a un funcionamiento eficaz para cualquier número de abonados, uno a varias centenas).
- Cobertura
  Técnicas avanzadas (Mesh, MIMO)
- Calidad del Servicio (Capa MAC con TDMA dinámico para soportar eficazmente servicios sensibles al retardo, tales como voz y video).
  Niveles de servicio diferenciados mediante asignación de ancho de banda.

Sin embargo, algunos estudios europeos y rusos recientes han encontrado que las estaciones que funcionan para trasmitir WiMax son nocivas para la salud y requieren de muchas especificaciones para evitar estos males a la sociedad, lamentablemente en México no contamos con normas relativas a estos deberes y los perjudicados en todo caso son los usuarios.

III.9 ¿Porqué WLAN – WiFi?

Ahora hay que tomar una decisión, ¿cuál tecnología es la que le conviene a la UNAM para implementar una red inalámbrica?

La decisión tomada es WiFi, por las siguientes razones:

- Costo de implementación económico
- Facilidad para operar junto a la RedUnam (cableada, backbone)
- Operación en bandas de frecuencia no licenciadas o libre
- Se basa en estándares internacionales
- El equipo para conectarse (tarjetas inalámbricas) es fácil de conseguir y a un precio cómodo.
- Buena velocidad de transmisión
- Puede usar WPA como método de seguridad
- Escalable

III.10 WLAN 802.11

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

WLAN 802.11b Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5,5 - 2 y 1 Mbit/s) y un alcance de 100 metros, que al igual que Bluetooth y Home RF, también emplea la banda de ISM de 2,4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH - Frequency Hopping), utiliza una la modulación linear compleja (DSSS). Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

WLAN 802.11g El IEEE también ha aprobado en el año 2003 en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión, también se le llama Wi-Fi.

WLAN 802.11a (Wi-Fi 5) El IEEE ratificó en julio de 1999 el estándar en 802.11a (los productos comerciales comienzan a aparecer a mediados del 2002), que con una modulación QAM-64 y la codificación OFDM (Orthogonal Frequency Division Multiplexing) alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros, lo que implica tener que montar más puntos de acceso (Access Points) que si se utilizase 802.11b para cubrir el mismo área, con el coste adicional que ello supone.
La banda de 5 GHz que utiliza se denomina UNII (Infraestructura de Información Nacional sin Licencia), que en los Estados Unidos está regulada por la FCC, el cual ha asignado un total de 300 MHz, cuatro veces más de lo que tiene la banda ISM, para uso sin licencia, en tres bloques de 100 MHz, siendo en el primero la potencia máxima de 50 mW, en el segundo de 250 mW, y en el tercero puede llegar hasta 1W, por lo que se reserva para aplicaciones en el exterior.

Estándar	Velocidad máxima	Interface de aire	Ancho de banda de canal	Frecuencia	Disponibilidad
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	Ahora
802.11ª	54 Mbps	OFDM	25 MHz	5.0 GHz	Ahora
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz	Ahora
HomeRF2	10 Mbps	FHSS	5 MHz	2.4 GHz	Ahora
HiperLAN2	54 Mbps	OFDM	25 MHz	5.0 GHz	Ahora
5-UP	108 Mbps	OFDM	50 MHz	5.0 GHz	Ahora
802.11n	600 Mbps		2 * 20 Mhz y 2* 40	2,4 y 5 Ghz simultáneamente	Enero 2007 (EU)

Tabla 5 Comparativa de estándares de WLAN

III.11 Seguridad

COMPATIBILIDAD Y SEGURIDAD. Wi-Fi y WEP

A finales de la década de los 90, los líderes de la industria inalámbrica (3Com, Aironet, Lucent, Nokia, etc.) crean la WECA (Wireless Ethernet Compatibility Alliance), una alianza para la Compatibilidad Ethernet Inalámbrica, cuya misión es la de certificar la interfuncionalidad y compatibilidad de los productos de redes inalámbricas 802.11b y promover este estándar para la empresa y el hogar.

Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricantes, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), y así los equipos con esta marca, soportada por más de 150 empresas, se pueden incorporar en las redes sin ningún problema, siendo incluso posible la incorporación de terminales telefónicos Wi-Fi a estas redes para establecer llamadas de voz.

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio, es la encriptación. En general se utiliza WEP (Wired Equivalent Privacy), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso.

La clave de acceso estándar es de 40 bits, pero existe otra opcional de 128 bits, y se asigna de forma estática o manual (no dinámica), tanto para los clientes, que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso a la red, lo que genera algunas dudas sobre su eficacia. WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado

Con el retraso del nuevo estándar 802.11i y con el fin de resolver el tema de la seguridad, se ha lanzado la certificación WPA, aunque algunos expertos consideran que esta es sólo una solución momentánea que puede llevar a error ya que puede crear en el usuario una sensación de seguridad que este estándar no ofrece.

Otro mecanismo de seguridad definido en el estándar IEE 802.11 es el conocido como SSID (Service Set Identifiers) o identificadores del conjunto de servicios, que es como un gestor de asignación de nombres, que proporciona un control de acceso muy rudimentario, razón por la que apenas se utiliza en las implementaciones comerciales.

Otros usuarios han preferido adquirir soluciones wireless convencionales y potenciar la seguridad con tecnología de otros fabricantes especializados en seguridad móvil en lugar de soluciones que incluyan la certificación WPA.

WEP

WEP, acrónimo de *Wired Equivalent Privacy*, 1999 - es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación *IV*) o de 128 bits (104 bits más 24 bits del IV).

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla (*seed* en inglés) para generar una secuencia de números pseudoaleatorios de mayor

tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado.

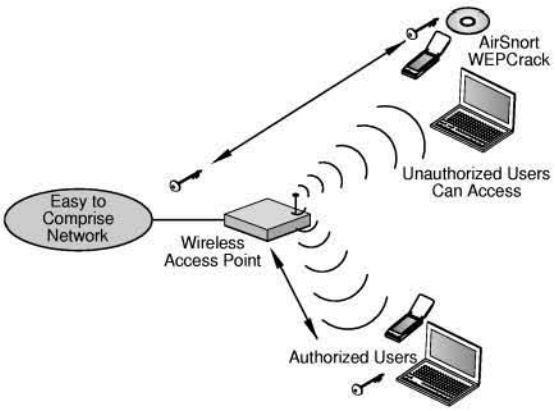
Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo RC4) para evitar secuencias iguales; de esta manera se crean nuevas semillas cada vez que varía.

Defectos

El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.

Para atacar una red Wi-Fi se suelen utilizar los llamados Packet sniffers y los *WEP Crackers*. Para llevar a cabo este ataque, se captura una cantidad de paquetes necesaria (dependerá del número de bits de cifrado) mediante la utilización de un Packet sniffer y luego mediante un WEP cracker o key cracker se trata de "romper" el cifrado de la red. Un key cracker es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Crackear una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.

A pesar de existir otros protocolos de cifrado mucho menos vulnerables y eficaces - como pueden ser el WPA o el WPA2- el protocolo WEP sigue siendo muy popular y posiblemente el más utilizado. Esto es debido a que WEP es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta. Sin embargo no ocurre lo mismo con otros protocolos como WPA, que no es soportado por mucho hardware antiguo. El hardware moderno pasa entonces a utilizar el modelo de seguridad WEP para poder interactuar con este hardware antiguo.



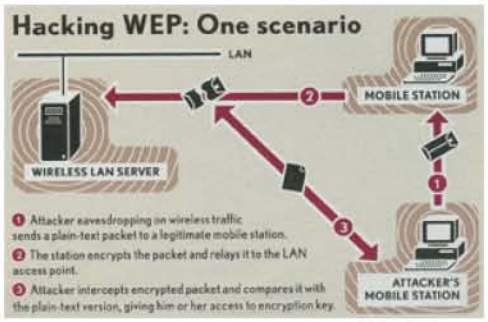


Figura 42. Hacking WEP

WPA

WPA (*Wi-Fi Protected Access* - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance"

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida ([PSK] - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

SSID

El **SSID** (**S**ervice **S**et **ID**entifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes *ad-hoc*, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (*Basic Service Set Identifier*); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el *broadcast* del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.

III.12 Evolución del Mercado

El mercado de las soluciones inalámbricas alcanzó en el año 2002 un volumen de negocio de unos 1.600 millones de dólares y según todas las previsiones, se espera que experimente un crecimiento anual del 20%, a pesar de algunos factores en su contra que frenan este desarrollo como los problemas de seguridad y la diversidad de estándares.

Y es que la preocupación por la seguridad es uno de los problemas que más tienen en cuenta las compañías, junto con las restricciones presupuestarias. A medida que la economía se vaya recuperando y los nuevos estándares incluyan características de seguridad mejorada, el mercado crecerá, por lo que se espera que en el año 2006 se alcance un volumen de 2.600 millones de dólares.

Otro de los factores negativos es que en este momento se está produciendo un retraso en el proceso de ratificación de los nuevos estándares. Este proceso, en el caso del 802.11i está siendo más caro y lento de lo que los fabricantes calcularon, por lo que hasta finales de 2003 o principios de 2004 este estándar no se lanzará al mercado.

Por otro lado, muchas compañías se han lanzado ya a comercializar soluciones que soportan el estándar 802.11g, aunque todavía no está definido del todo. Las primeras pruebas con este tipo de equipos han demostrado que la interoperabilidad presenta lagunas, y que en redes híbridas, las prestaciones tienden a caer a los niveles del estándar anterior.

Se espera que el crecimiento venga impulsado por la tecnología Wi-Fi, así como por la mayor presencia de las tarjetas multiprotocolo, capaces de operar en estándares diversos como el 802.11b a, b y g. De hecho, en Estados Unidos esto ya se está produciendo ya que el protocolo 802.11b, convive con el 802.11a, que ofrece un mayor ancho de banda. Además, esta opción tiene la ventaja de proteger las inversiones de la obsolescencia y permite administrar el ancho de banda en función del uso o localizaciones.

La evolución del mercado de la movilidad vendrá dada sin lugar a dudas por tres "actores" fundamentales en este mercado: los dispositivos móviles, las redes wireless y las aplicaciones móviles. De los primeros podemos decir que cada vez son más potentes y para los próximos años se espera que las PC incorporen plataformas y tecnologías móviles y los portátiles se acerquen cada vez más al PC, hasta que compartan la misma tecnología. Se espera que esto mismo ocurra con el resto de dispositivos móviles, que converjan poco a poco hacia la compatibilidad total con el PC, a medida que su capacidad vaya incrementándose. Y por otro lado aparecerán nuevos dispositivos móviles que se adaptarán mejor a las necesidades de cada tipo de empresa.

Por su parte, según la consultora Ciga Group, las redes wireless van a evolucionar de diferente manera: a través de la consolidación de redes de tercera generación, gracias a los cambios en el ancho de banda y la cobertura de las redes, etc. Sin embargo existe la amenaza de la interrelación de los diferentes estándares y tecnologías, lo que podría hacer que las empresas tuvieran que elegir entre una tecnología concreta o tecnologías que permitan utilizar diferentes redes, a costa de una mayor complejidad y precios.

Por último podemos decir que tanto la mejora de las redes como una mayor capacidad permitirán montar redes con dispositivos-clientes móviles siempre conectados, de igual

manera a como sucede en las redes móviles de 2.5G GSM/GPRS, al tiempo que habrá un despliegue de Web Services para aplicaciones móviles.

El informe también apunta que una serie de facilidades y ventajas de estas tecnologías van a hacer posible la rápida expansión de estas aplicaciones móviles como por ejemplo la ubicuidad, la incorporación a los PC de tecnología Wi-Fi de serie, la mejora de los estándares de seguridad, etc. Y una tendencia importante sería la aparición de una plataforma de conmutación centralizada que integra capacidades para gestionar la seguridad, la administración de la red y la calidad de servicio.

En cuanto a las tendencias tecnológicas se está trabajando con el fin de ofrecer soluciones inalámbricas con puntos de acceso más ligeros y económicos y con una plataforma que permita controlarlos de forma centralizada, además de incorporar otras funcionalidades.

IV. RIU

IV.1 ¿Qué es la RIU?

La Red Inalámbrica Universitaria es una red de puntos de acceso (APs) instalados a lo largo de Ciudad Universitaria que basan su funcionamiento en los protocolos de comunicación 802.11a, 802.11g y 802.11b ó Wi-Fi. La RIU es un complemento de la red alambrada RedUNAM que permite el acceso a la Internet proveyendo movilidad para la comunidad estudiantil y académica universitaria. Es decir, es un intento por parte de la UNAM para integrarse al concepto de NGN.

La RIU usa ondas de radio para enviar y recibir datos. Como en cualquier otra red inalámbrica, tanto los dispositivos móviles como los puntos de acceso (APs) convierten la información digital (1s y 0s) en ondas de radio lo que permite su transmisión usando el aire como medio de transporte.

La RIU opera bajo bandas de frecuencias no licenciadas o libres como son la 5.7 GHz y 2.4GHz basándose en los estándares internacionales de redes inalámbricas de área local 802.11a, 802.11b y 802.11g.

Para estar en posibilidad de usar la red, es preciso contar con un dispositivo portátil como una Lap Top que cuente con tarjetas de acceso inalámbrico compatibles con la red. Los estándares de comunicación soportados son 802.11a, 802.11b y 802.11g. En cuanto a seguridad el protocolo soportado es WPA.

IV.2 Características de la RIU

Objetivo

La Red Inalámbrica Universitaria es la red que permite la navegación por Internet con el uso de dispositivos móviles como Lap Tops a través de CU, tiene por objetivo proveer acceso a Internet y sus aplicaciones a través del campus universitario como complemento a la RedUNAM, permitiendo así movilidad y mayor flexibilidad a sus usuarios.

Cobertura

La red ha iniciado su cobertura en la zona de las Islas e irá ampliándose paulatinamente a través del campus, por lo que para el principio de 2006 cubrirá a más de 40 escuelas, facultades, institutos y centros de investigación en Ciudad Universitaria.

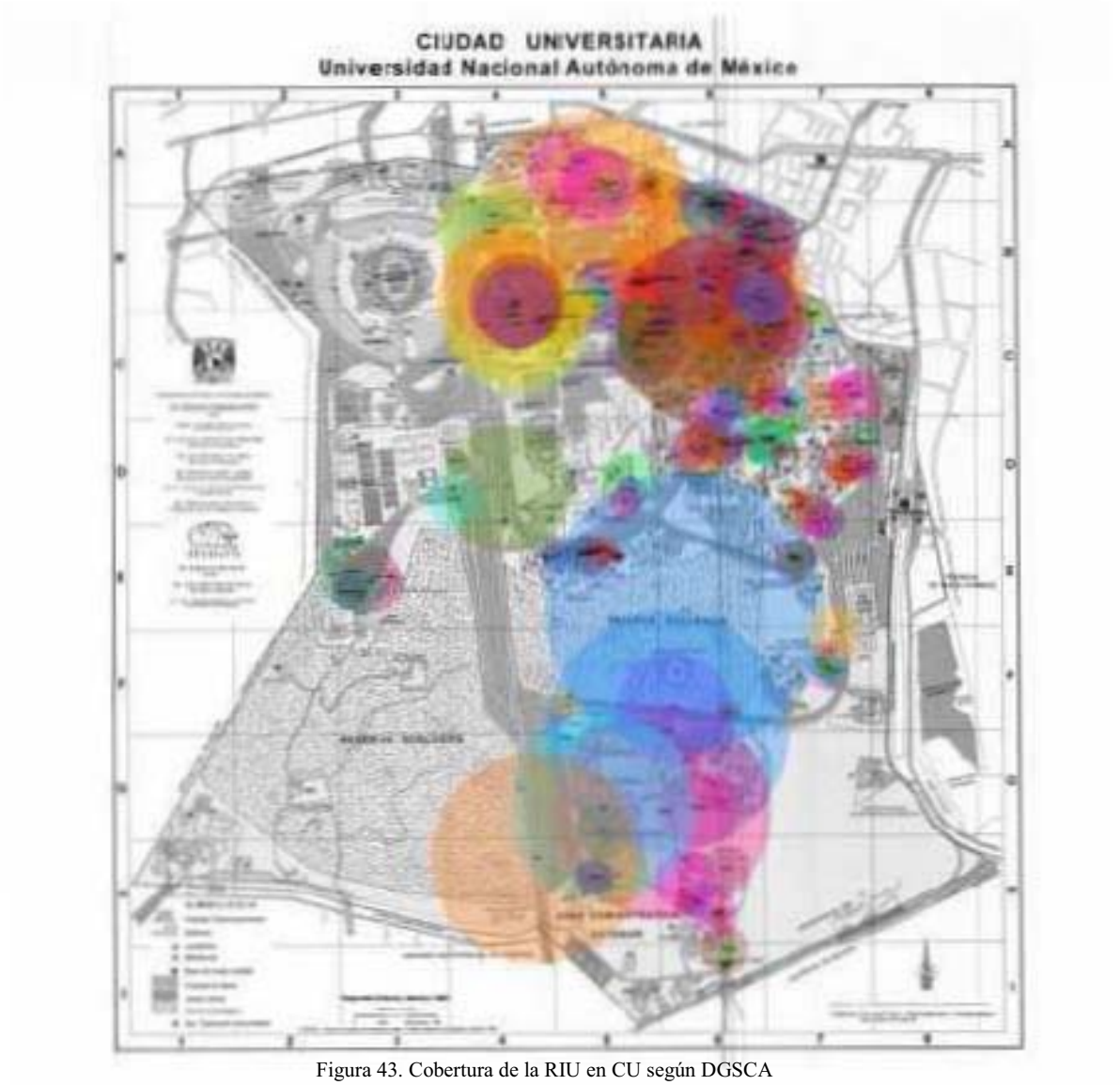


Figura 43. Cobertura de la RIU en CU según DGSCA

Figura 44. Access Points en Ciudad Universitaria

Dependencias universitarias que estarán en cobertura para enero de 2006

Biblioteca Central
Biblioteca Nacional
Centro de Ciencias de la Atmósfera
Centro de Ecología
Centro de Enseñanza de Lenguas Extranjeras
Centro de Enseñanza para Extranjeros
Centro Coordinador y Difusor de Estudios Latinoamericanos
Centro de Investigación sobre América del Norte
Centro de Investigación Interdisciplinario en Ciencias y Humanidades

Centro Universitario de Investigaciones Bibliotecológicas
Coordinación de Humanidades
Coordinación de la Investigación Científica
Dirección General de Servicios de Cómputo Académico
Escuela Nacional de Trabajo Social
Facultad de Arquitectura
Facultad de Ciencias
Facultad de Ciencias Políticas
Facultad de Contaduría y Administración
Facultad de Derecho
Facultad de Economía
Facultad de Filosofía y Letras
Facultad de Ingeniería
Facultad de Medicina
Facultad de Medicina Veterinaria y Zootecnia
Facultad de Odontología
Facultad de Psicología
Facultad de Química
Instituto de Astronomía
Instituto de Biología
Instituto de Ciencias Nucleares
Instituto de Economía
Instituto de Fisiología Celular
Instituto de Geofísica
Instituto de Geografía
Instituto de Geología
Instituto de Investigación en Matemáticas Aplicadas y Sistemas
Instituto de Investigaciones Antropológicas
Instituto de Investigaciones Biomédicas
Instituto de Investigaciones Estéticas
Instituto de Investigaciones Históricas
Instituto de Investigaciones Jurídicas
Instituto de Investigaciones Sociales
Instituto de Matemáticas
Instituto de Investigaciones en Materiales
Instituto de Química
Jardín Botánico
Unidad de Seminarios
Universum

Tabla 6. Dependencias Universitarias con cobertura de RIU

Velocidad

La RIU como cualquier red inalámbrica basa su comunicación en la transmisión de ondas de radio frecuencia entre la tarjeta de red y el punto de acceso (AP).

Estas señales no son inmunes a la interferencia de otros dispositivos inalámbricos y pudieran no penetrar adecuadamente a través de ciertos materiales. Debido a estas

condiciones, las velocidades, la recepción y la distancia al punto de acceso variarán con respecto a las especificadas en los estándares. Las velocidades esperadas pueden ser para los estándares 802.11 a y g de 6 a 54Mbps y para el estándar 802.11 b de 2 a 11Mbps.

¿Cuál es la distancia a la que debe estar un dispositivo móvil para conectarse a un AP?

La distancia para una conexión efectiva con un AP depende de muchos factores entre los que destacan la interferencia de otros dispositivos y las obstrucciones físicas (paredes, libreros, etc.). Con las condiciones adecuadas, si la conexión es al aire libre con línea de vista al AP, la conexión puede lograrse en 80m o más. En áreas cerradas, se puede lograr conexión a una distancia de 40 o 50m.

La seguridad en una red inalámbrica es un punto crucial ya que no sólo es un medio que se comparte con otros usuarios, a diferencia del cable que conecta nuestra computadora personal en el escritorio, sino que además es un medio que transmite ondas de radio por el aire a frecuencias que pueden ser captadas por otros dispositivos operando en las mismas frecuencias. Esto es, la información en una red inalámbrica por su misma naturaleza se puede considerar no segura. Para proteger la información se recomienda utilizar aplicaciones seguras tanto para navegar como para transmitir archivos como lo son SSL y SSH. La RIU tiene como característica el uso del protocolo WPA que permite una mayor seguridad para el acceso a los usuarios y el cifrado de su información.

¿Qué es WPA? ¿Se usa en la RIU?

Wi-Fi Protected Access es un estándar desarrollado para aumentar la seguridad de la información así como el control de acceso de los usuarios. La RIU utiliza WPA como protocolo de cifrado para la protección de la información asegurando que sólo usuarios autorizados pueden hacer uso de la infraestructura.

¿Qué es WEP? ¿Se usa en la RIU?

Wired Equivalent Privacy es un método de cifrado para la seguridad de las redes inalámbricas, sin embargo, por la debilidad del algoritmo que puede ser descifrado relativamente fácil, no se aplica en la RIU.

¿Otros dispositivos inalámbricos pueden interferir con las señales de la RIU?

Sí, como cualquier red inalámbrica, otros dispositivo que opere en las frecuencias de 2.4GHz y 5.8GHz cerca de los dispositivos de conexión a la RIU pueden afectar el desempeño de la conexión e incluso terminarla. Dispositivos que operan en estas frecuencias, particularmente la 2.4GHz son teléfonos inalámbricos, hornos de microondas, cámaras y otros dispositivos.

Arquitectura y Topología

La RIU tiene una arquitectura centralizada, lo que permite controlar todos los AP´s por medio de un dispositivo central, la asignación de perfiles que simulan una Service Class en donde se encuentra información de la cuenta, nombre, servicios, etc.

Como desventaja de esta arquitectura es que el buen funcionamiento de los AP´s depende en buena medida del central.

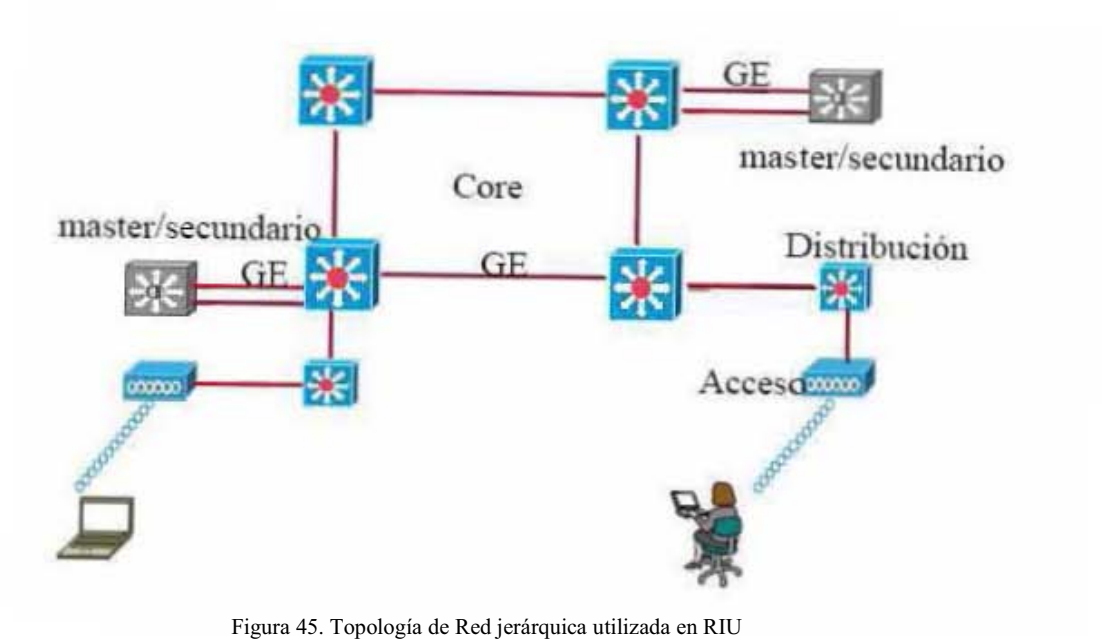


Figura 45. Topología de Red jerárquica utilizada en RIU

Direccionamiento

- RFC 1918 (IP)
- DHCP
- Subnetting

RIU Monitoreo

- SNMPv2
- AP´s Asociados
- Usuarios Asociados
- Tráfico por AP, por switch
- Manejo de Traps

Política de uso

- Usuarios
- Prestación del servicio
- Disponibilidad del Servicio
- Cobertura
- Usos Prohibidos
- Sanciones
- Monitoreo de la Red

Análisis de Riesgos

Permite identificar las amenazas potenciales, tecnológicas o humanas, que pongan en peligro la operación de la red, es importante ya que en buena medida se basa el diseño de la arquitectura en la seguridad de la red.

- Ataque pasivo de captura de tráfico (sin cifrado)
- Ataque pasivo para romper el cifrado WEP
- Ataque pasivo para romper el cifrado WPA

- Ataque de sniffing
- Evil twin (Gemelo maligno)
- Propagación de código malicioso
- Uso simultáneo de cuentas de usuario
- Otros muchos ataques
- Interferencia con otras redes
- Interferencia con otros dispositivos funcionando en la frecuencia de los 2.4 GHz, ejemplo bluetooth
- Condiciones climáticas
- Límites físicos

V. WLAN en la Facultad de Ingeniería

V.1 Cobertura en los edificios de la F.I.

Anexo de Ingeniería

Tabla 7. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	WEP
IVirtual	2/5	WEP
Diedimei2A	2/5	Red no segura
Diedimei2G	2/5	Red no segura
Red sin nombre	2/5	WEP

Figura 46. Anexo de Ingeniería 1

Tabla 8. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	WEP
IVirtual	2/5	WEP
Diedimei2A	3/5	Red no segura
Imsr WiFi	2/5	Red no segura
LINDA	3/5	Red no segura
hpsetup	2/5	Red no segura

Red sin nombre	3/5	WEP
Diedimei2G	3/5	Red no segura

Tabla 9. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	3/5	Red no segura
Mobilean	3/5	WEP
Red LPDI	1/5	WPA – PSK
IVirtual	1/5	WEP
Diedimei2A	2/5	Red no segura
Imsr WiFi	3/5	Red no segura
LINDA	4/5	Red no segura
Red sin nombre	3/5	WEP
Diedimei2G	3/5	Red no segura

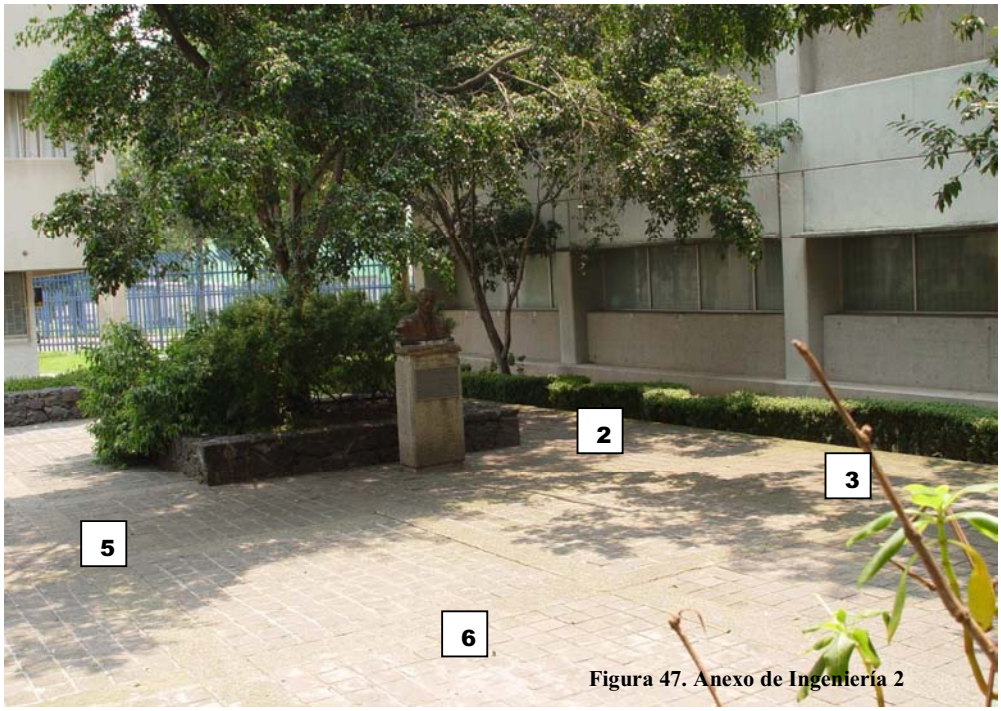


Figura 47. Anexo de Ingeniería 2

Tabla 10. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 4

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	3/5	WEP
IVirtual	1/5	WEP
Diedimei2A	3/5	Red no segura
Imsr WiFi	3/5	Red no segura
LINDA	3/5	Red no segura
Diedimei2G	4/5	Red no segura
Red sin nombre	2/5	WEP
MEMs	2/5	WEP

Tabla 10. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 5

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	3/5	Red no segura
Mobilean	3/5	WEP
PAEFI	1/5	WEP
IVirtual	2/5	WEP
Diedimei2A	3/5	Red no segura
Imsr WiFi	2/5	Red no segura
LINDA	3/5	Red no segura
Diedimei2G	4/5	Red no segura
Red sin nombre	2/5	WEP
MEMs	2/5	WEP

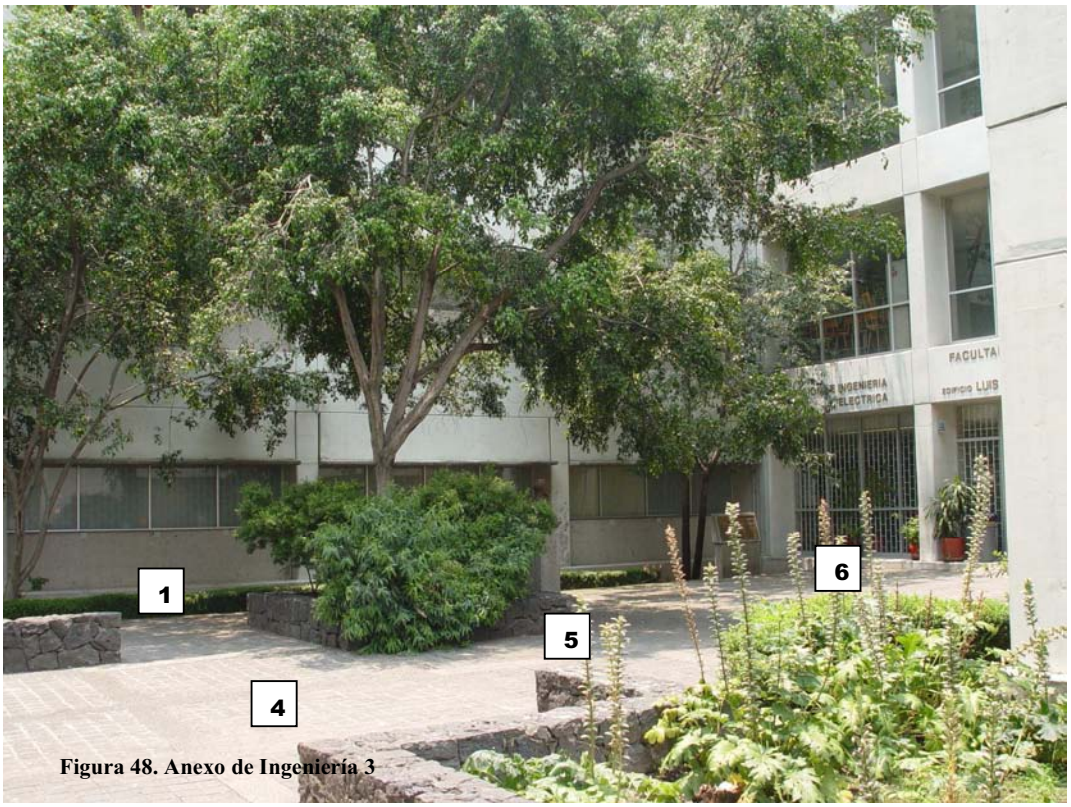


Figura 48. Anexo de Ingeniería 3

Tabla 11. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 6

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	3/5	Red no segura
Mobilean	3/5	WEP
PAEFI	1/5	WEP
IVirtual	1/5	WEP
Diedimei2A	4/5	Red no segura
Imsr WiFi	3/5	Red no segura
LINDA	2/5	Red no segura
Diedimei2G	5/5	Red no segura
Red sin nombre	3/5	WEP

Red LPDI	3/5	WPA – PSK

Tabla 12. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 7

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	WEP
PAEFI	1/5	WEP
IVirtual	2/5	WEP
Diedimei2A	3/5	Red no segura
Imsr WiFi	4/5	Red no segura
LINDA	2/5	Red no segura
Diedimei2G	2/5	Red no segura

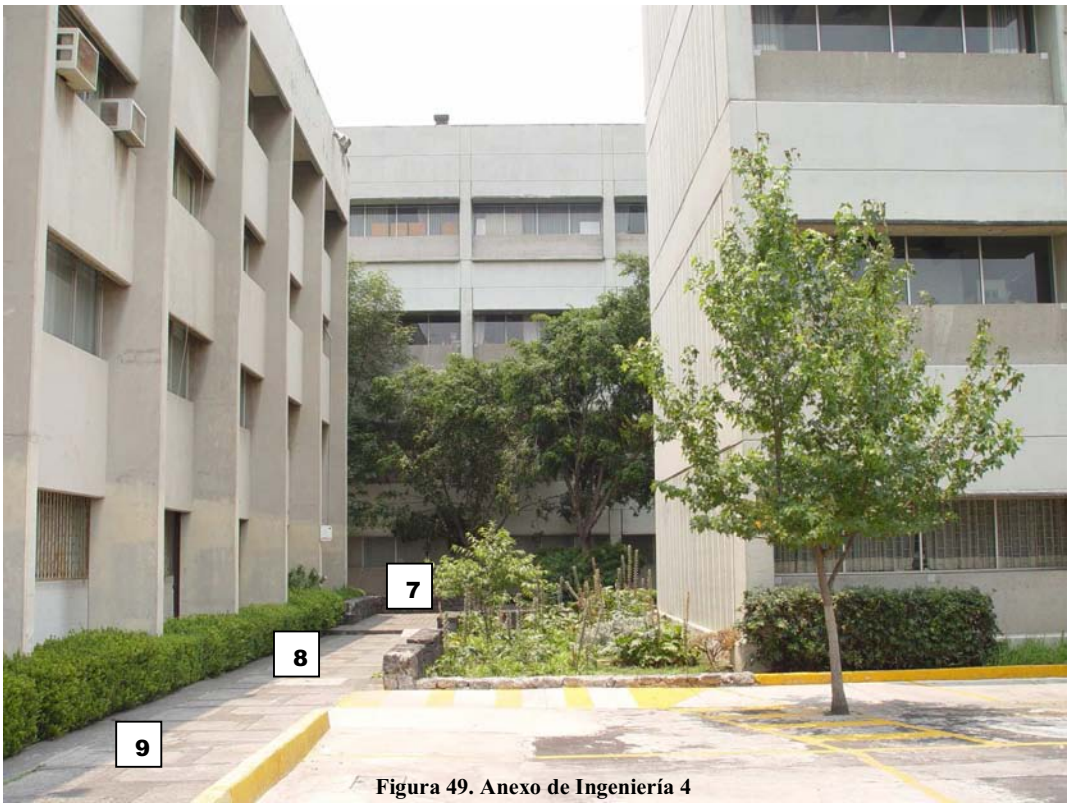


Figura 49. Anexo de Ingeniería 4

Tabla 13. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 8

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	WEP
PAEFI	2/5	WEP
IVirtual	2/5	WEP
Diedimei2A	2/5	Red no segura
Imsr WiFi	3/5	Red no segura
LINDA	4/5	Red no segura
Diedimei2G	2/5	Red no segura
MEMs	2/5	WEP

LAB_SIMULACION	2/5	WPA – PSK
Antena1	1/5	WEP

Tabla 14. Anexo de Ingeniería. Espacio enfrente del edificio Valdés Vallejo 9

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Mobilean	2/5	Red no segura
Imsr WiFi	3/5	WEP
IVirtual	3/5	WEP
LINDA	2/5	Red no segura
PAEFI	3/5	WEP
LAB SIMULACION	2/5	WPA – PSK
Red sin nombre	2/5	WEP

Edificio Valdés Vallejo

Tabla 15. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso0. Medición1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	3/5	Red no segura
Mobilean	2/5	Red no segura
Diedimei2A	4/5	Red no segura
Imsr WiFi	3/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	3/5	Red no segura
LPDI	2/5	WPA – PSK

Figura 50. Anexo de Ingeniería 5

Tabla 16. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso0. Medición2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	Red no segura
Diedimei2A	4/5	Red no segura
Imsr WiFi	3/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	3/5	Red no segura

Tabla 17. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso0. Medición3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	Red no segura
Diedimei2A	4/5	Red no segura
Imsr WiFi	2/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	5/5	Red no segura

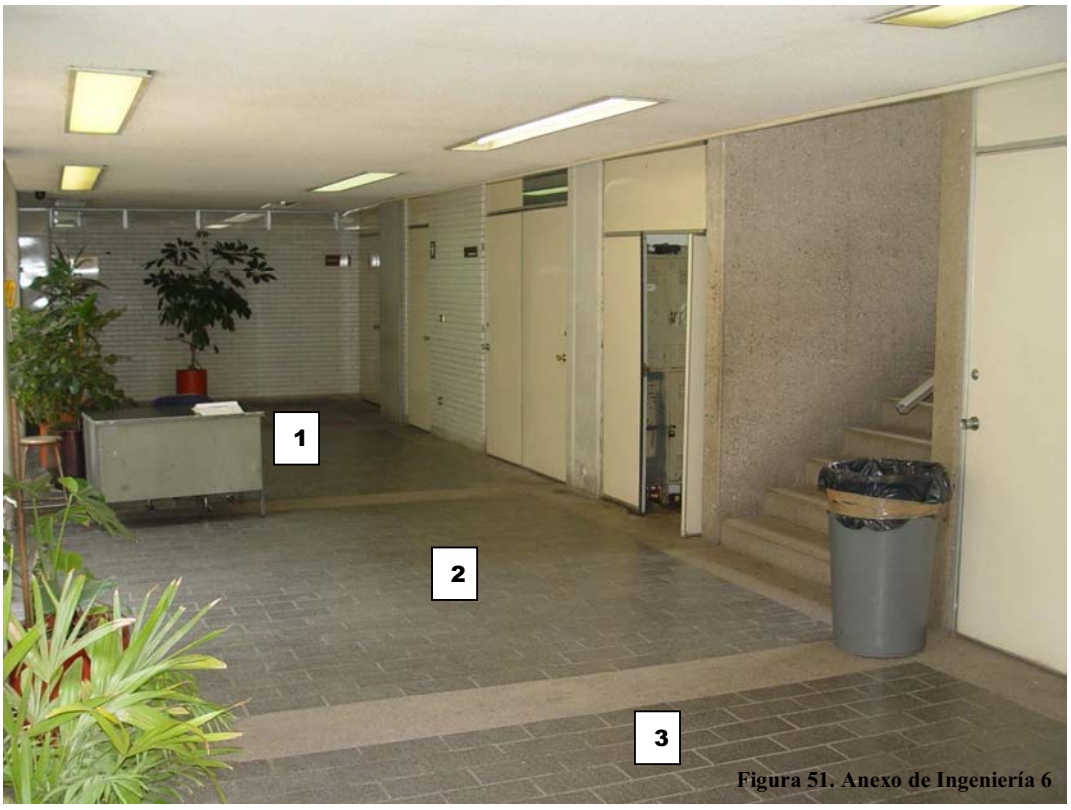


Figura 51. Anexo de Ingeniería 6

Tabla 18. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso1. Medición1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	Red no segura
Diedimei2A	2/5	Red no segura

Imsr WiFi	3/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	2/5	Red no segura

Figura 52. Anexo de Ingeniería 7

Tabla 19. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso1. Medición 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	2/5	Red no segura
IVirtual	2/5	WEP
Diedimei2A	2/5	Red no segura
Imsr WiFi	3/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	3/5	Red no segura
ROBOCUP	2/5	Red no segura
Antena_1	2/5	WEP
Linksys	1/5	Red no segura

Tabla 20. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso1. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	1/5	Red no segura
Mobilean	2/5	Red no segura
Diedimei2A	2/5	Red no segura
Imsr WiFi	2/5	WEP
LINDA	2/5	Red no segura

Diedimei2G	1/5	Red no segura

Figura 53. Anexo de Ingeniería 8

Tabla 21. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 2. Medición 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab. Redes	2/5	Red no segura
Mobilean	3/5	Red no segura
PAEFI	2/5	WEP
IVirtual	1/5	WEP
Imsr WiFi	4/5	WEP
Diedimei2G	1/5	Red no segura
MEMs	2/5	WEP
ROBOCUP	2/5	Red no segura
Mobilecom	2/5	Red no segura

Figura 54. Anexo de Ingeniería 9

Tabla 22. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 2. Medición 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LPDI	2/5	WPA – PSK
Mobilean	3/5	Red no segura
PAEFI	1/5	WEP
UVMU4-Biblioteca1	3/5	Red no segura
Imsr WiFi	3/5	WEP
Diedimei2G	2/5	Red no segura
ROBOCUP	2/5	Red no segura
Mobilecom	2/5	Red no segura
Lab_voz	1/5	Red no segura
Linksys	2/5	Red no segura

Tabla 23. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 2. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
IVirtual	2/5	WEP
Mobilean	3/5	Red no segura
PAEFI	1/5	WEP
UVMU4-Biblioteca1	1/5	Red no segura
Imsr WiFi	4/5	WEP
Diedimei2G	2/5	Red no segura
Linksys	1/5	Red no segura

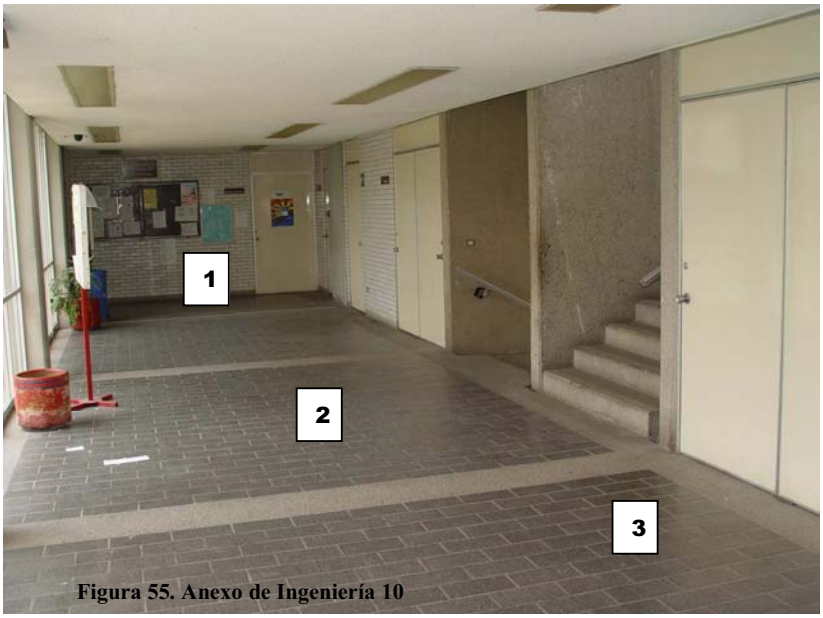


Figura 55. Anexo de Ingeniería 10

Tabla 24. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 3. Medición 1

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
IVirtual	1/5	Red no segura
Mobilean	5/5	Red no segura
PAEFI	1/5	WEP
UVMU4-Biblioteca1	3/5	Red no segura
Imsr WiFi	4/5	WEP
Diedimei2G	1/5	Red no segura
Mobilecam	3/5	Red no segura
Trino	1/5	WEP
LINDA	1/5	Red no segura

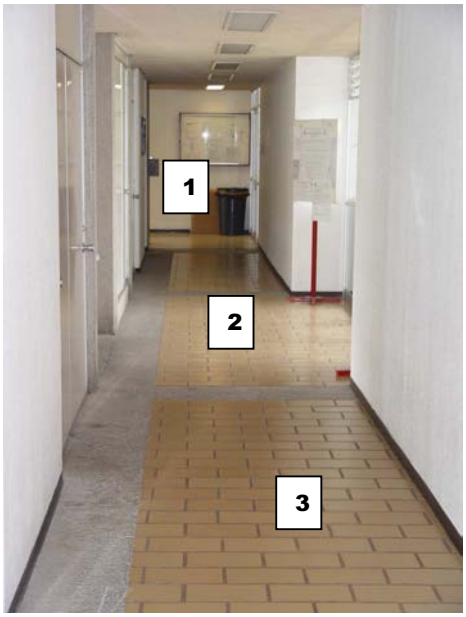


Figura 56. Anexo de Ingeniería 11

Tabla 25. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 3. Medición 2

RED	Intensidad	Seguridad
RIU	2/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LDPI	1/5	WPA – PSK
Mobilean	3/5	Red no segura
Lab_voz	2/5	Red no segura
Imsr WiFi	1/5	WEP
Mobilecam	1/5	Red no segura

Tabla 26. Anexo de Ingeniería. Edificio Valdés Vallejo. Piso 3. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Mobilean	3/5	Red no segura
Imsr WiFi	2/5	WEP
Trino	2/5	WEP
ROBOCUP	2/5	Red no segura
PAEFI	2/5	WEP
Linksys	2/5	Red no segura

Espacio que rodea a la División de Ingeniería Mecánica e Industrial (MEMDimei)

Tabla 27. Anexo de Ingeniería. Espacio que rodea la MEMDimei 1

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Red sin nombre	2/5	WEP
2WIREFINAL	2/5	WEP

Tabla 28. Anexo de Ingeniería. Espacio que rodea la MEMDimei 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
IVirtual	1/5	Red no segura
2WIREFINAL	2/5	WEP

Tabla 29. Anexo de Ingeniería. Espacio que rodea la MEMDimei 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	2/5	WEP

Tabla 30. Anexo de Ingeniería. Espacio que rodea la MEMDimei 4

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	2/5	WEP
PAEFI	1/5	WEP

Figura 57. Anexo de Ingeniería 12

Figura 58. Anexo de Ingeniería 13

Tabla 31. Anexo de Ingeniería. Espacio que rodea la MEMDimei 5

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	2/5	WEP
Diedimei2G	1/5	Red no segura

Tabla 32. Anexo de Ingeniería. Espacio que rodea la MEMDimei 6

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
PAEFI	2/5	WEP
IVirtual	2/5	WEP

Tabla 33. Anexo de Ingeniería. Espacio que rodea la MEMDimei 7

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Mobilean	2/5	WEP
Imsr WiFi	3/5	WEP
IVirtual	3/5	WEP
LINDA	2/5	Red no segura
PAEFI	3/5	WEP
LAB SIMULACION	2/5	WPA – PSK
Red sin nombre	2/5	WEP

Figura 59. Anexo de Ingeniería 14

Tabla 34. Anexo de Ingeniería. Espacio que rodea la MEMDimei 10

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	1/5	WEP
Diedimei2G	1/5	Red no segura

Tabla 35. Anexo de Ingeniería. Espacio que rodea la MEMDimei 11

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
PAEFI	1/5	WEP
IVirtual	2/5	WEP

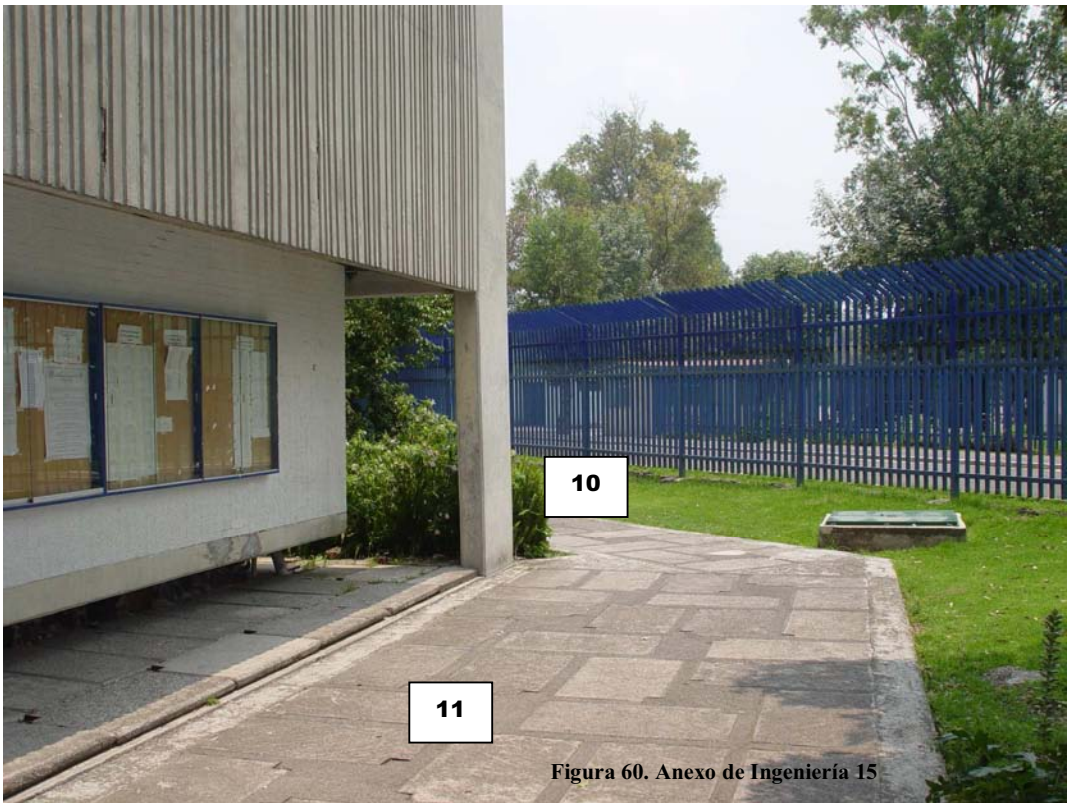


Figura 60. Anexo de Ingeniería 15

Tabla 36. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 0. Medición 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura
PAEFI	1/5	WEP
Diedimei2G	1/5	Red no segura

Tabla 37. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 0. Medición 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura

PAEFI	2/5	WEP
Red sin nombre	2/5	WEP
Diedimei2G	1/5	Red no segura

Tabla 38. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 0. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura
PAEFI	1/5	WEP
Red sin nombre	2/5	WEP
Diedimei2G	1/5	Red no segura

Tabla 39. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 0. Medición 4

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura
PAEFI	2/5	WEP
Red sin nombre	3/5	WEP
Antena_1	1/5	WEP

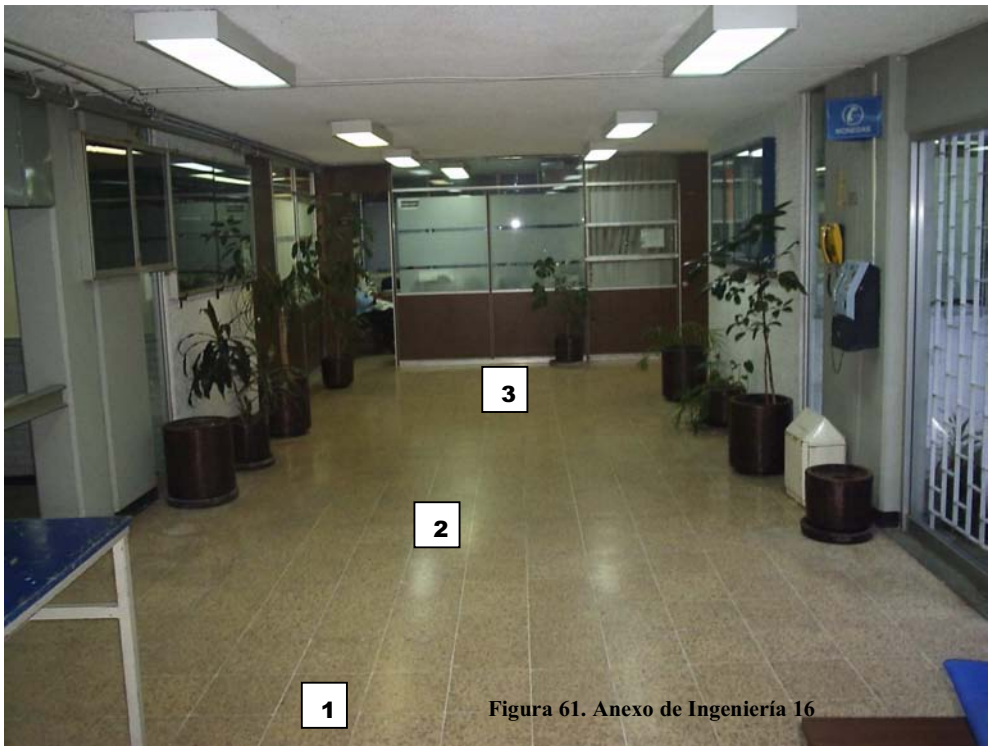


Figura 61. Anexo de Ingeniería 16

Tabla 40. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 0. Medición 5

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura
PAEFI	2/5	WEP
Red sin nombre	3/5	WEP
IVirtual	2/5	WEP
Imsr WiFi	2/5	WEP

LAB SIMULACION	2/5	WPA – PSK
2WIREFINAL	2/5	WEP
Antena_1	1/5	WEP

Tabla 41. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 1. Medición 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
LINDA	2/5	Red no segura
2WIREFINAL	2/5	WEP
Diedimei2G	1/5	Red no segura
Red sin nombre	1/5	WEP

Tabla 42. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 1. Medición 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
PAEFI	2/5	WEP
2WIREFINAL	1/5	WEP
Diedimei2G	2/5	Red no segura
Red sin nombre	1/5	WEP

Tabla 43. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 1. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
PAEFI	1/5	WEP
2WIREFINAL	2/5	WEP
Diedimei2G	1/5	Red no segura
Red sin nombre	1/5	WEP

Tabla 44. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 1. Medición 4

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
PAEFI	1/5	WEP
LINDA	2/5	Red no segura
Diedimei2G	1/5	Red no segura

Tabla 45. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 1. Medición 5

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	2/5	WEP
Diedimei2G	1/5	Red no segura

Figura 62. Anexo de Ingeniería 17

Tabla 46. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 2. Medición 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	1/5	WEP
Diedimei2G	2/5	Red no segura
Imsr WiFi	2/5	WEP
IVirtual	1/5	WEP

Tabla 47. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 2. Medición 2

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
2WIREFINAL	1/5	WEP
Diedimei2G	2/5	Red no segura
Imsr WiFi	2/5	WEP
IVirtual	1/5	WEP

Tabla 48. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 2. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
MEMs	2/5	WEP
IVirtual	3/5	WEP
PAEFI	2/5	WEP
Imsr WiFi	1/5	WEP

Tabla 49. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 2. Medición 4

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)

MEMs	3/5	WEP
IVirtual	2/5	WEP
PAEFI	2/5	WEP
Imsr WiFi	1/5	WEP

Tabla 50. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 3. Medición 1

RED	**Intensidad**	**Seguridad**
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
MEMs	4/5	WEP
IVirtual	3/5	WEP

Tabla 51. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 3. Medición 2

RED	**Intensidad**	**Seguridad**
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
MEMs	5/5	WEP
IVirtual	2/5	WEP

Tabla 52. Anexo de Ingeniería. Edificio DIE-DIMEI. Piso 3. Medición 3

RED	**Intensidad**	**Seguridad**
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
MEMs	5/5	WEP
IVirtual	2/5	WEP

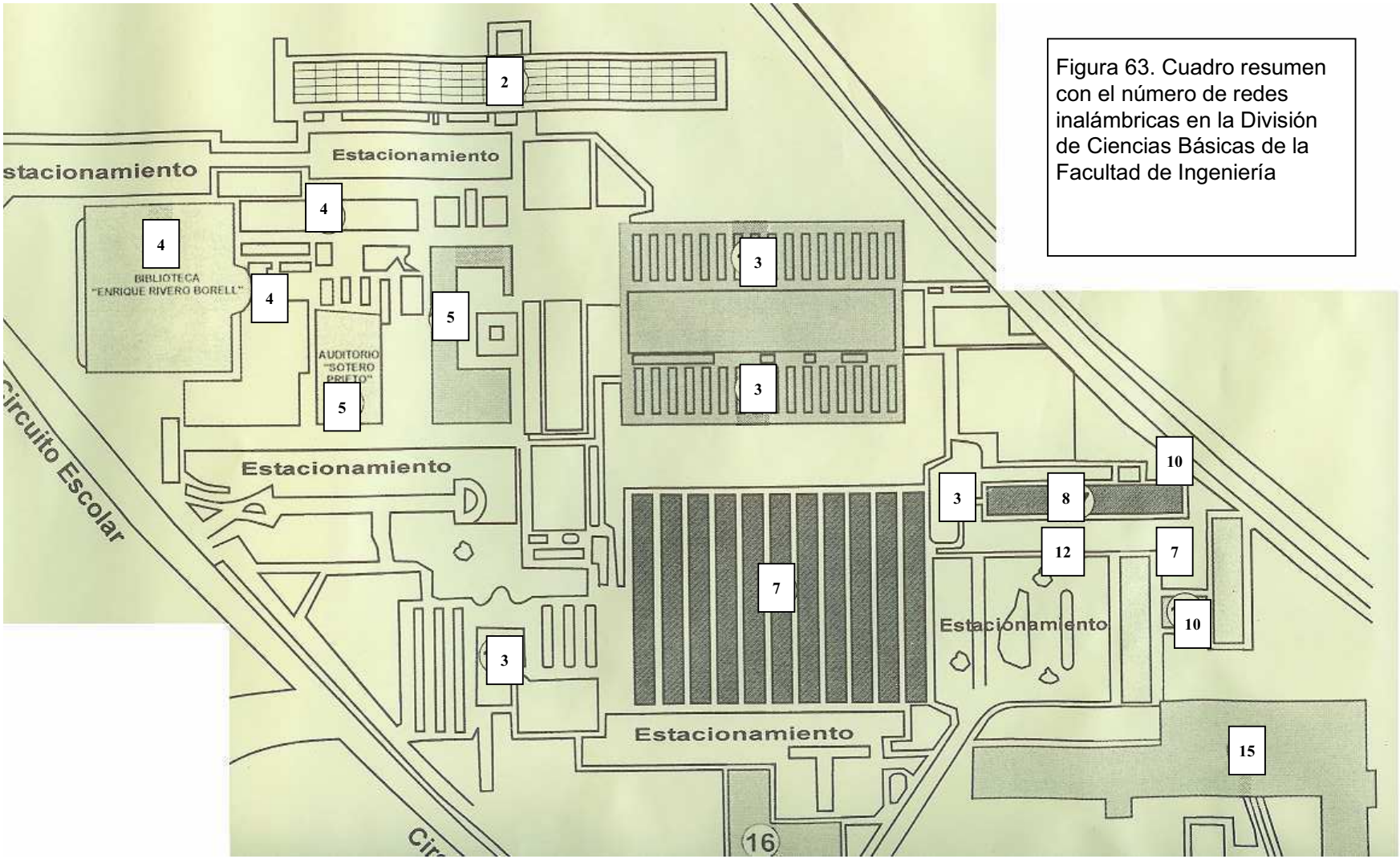


Figura 63. Cuadro resumen con el número de redes inalámbricas en la División de Ciencias Básicas de la Facultad de Ingeniería

Facultad de Ingeniería

Tabla 53. Facultad de Ingeniería. Medición 1

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	2/5	Red no segura
hpsetup	1/5	WEP
riu	1/5	WEP

Tabla 54. Facultad de Ingeniería. Medición 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	4/5	WEP
Red sin nombre	2/5	Red no segura

Tabla 55. Facultad de Ingeniería. Medición 3

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	4/5	WEP
hpsetup	2/5	WEP
Red sin nombre	2/5	Red no segura

Tabla 56. Facultad de Ingeniería. Medición 4

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	1/5	Red no segura

Tabla 57. Facultad de Ingeniería. Medición 5

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	2/5	Red no segura

Tabla 58. Facultad de Ingeniería. Medición 6

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	1/5	Red no segura

Tabla 59. Facultad de Ingeniería. Medición 7

RED	Intensidad	Seguridad
RIU	2/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	3/5	WEP

Figura 63. Facultad de Ingeniería 1

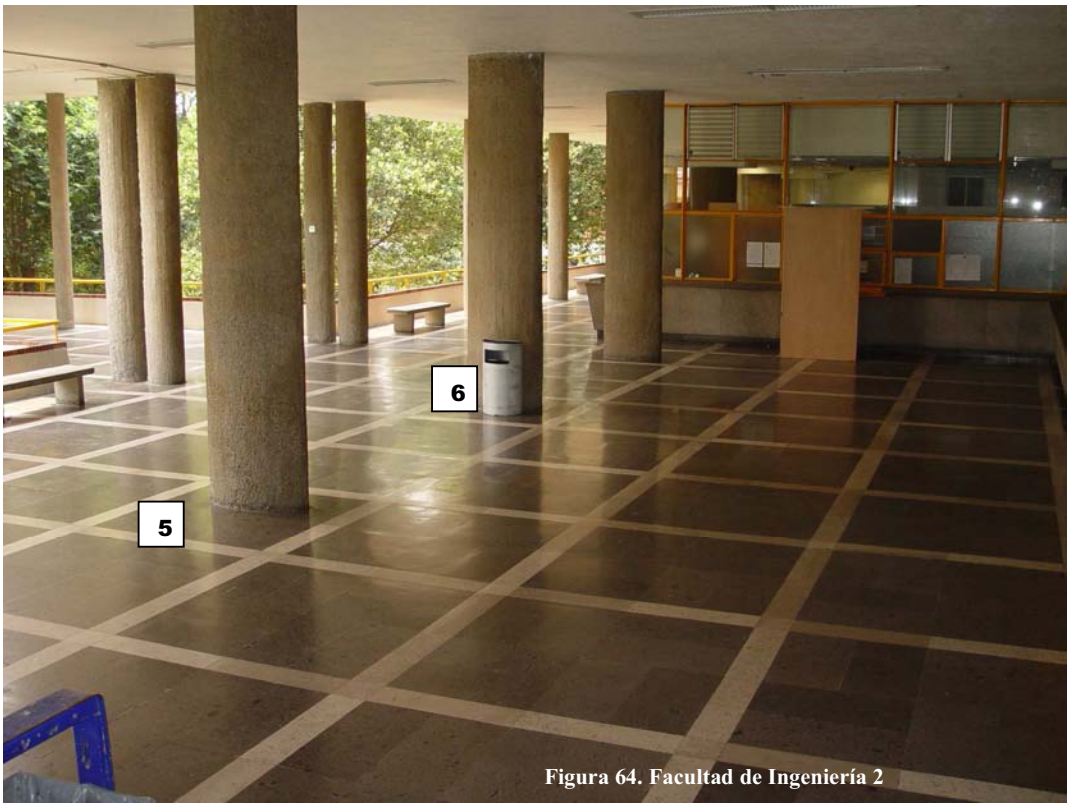


Figura 64. Facultad de Ingeniería 2

Tabla 60. Facultad de Ingeniería. Planta baja 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	1/5	WEP
Red sin nombre	1/5	Red no segura

Tabla 61. Facultad de Ingeniería. Planta baja 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	1/5	Red no segura

Figura 65. Facultad de Ingeniería 3

Tabla 62. Facultad de Ingeniería. Planta baja 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	1/5	WEP

Tabla 63. Facultad de Ingeniería. Planta baja 4

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	1/5	WEP
Red sin nombre	2/5	Red no segura

Jardines

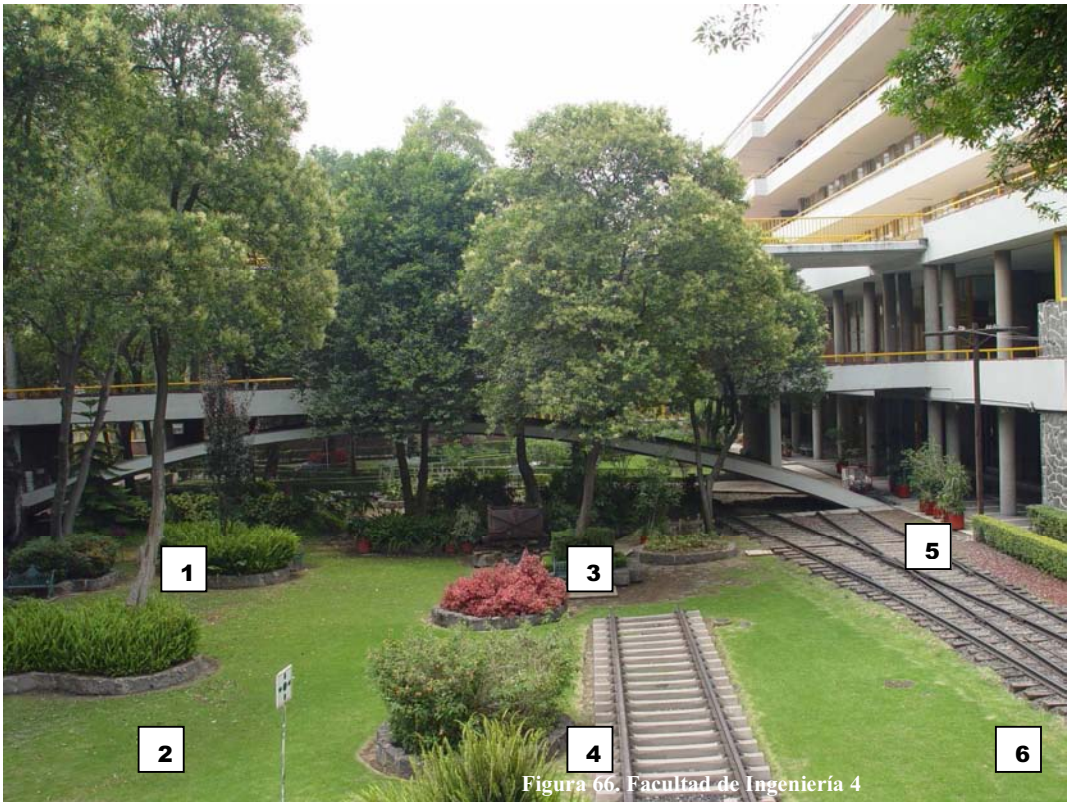


Figura 66. Facultad de Ingeniería 4

Figura 67. Facultad de Ingeniería 5

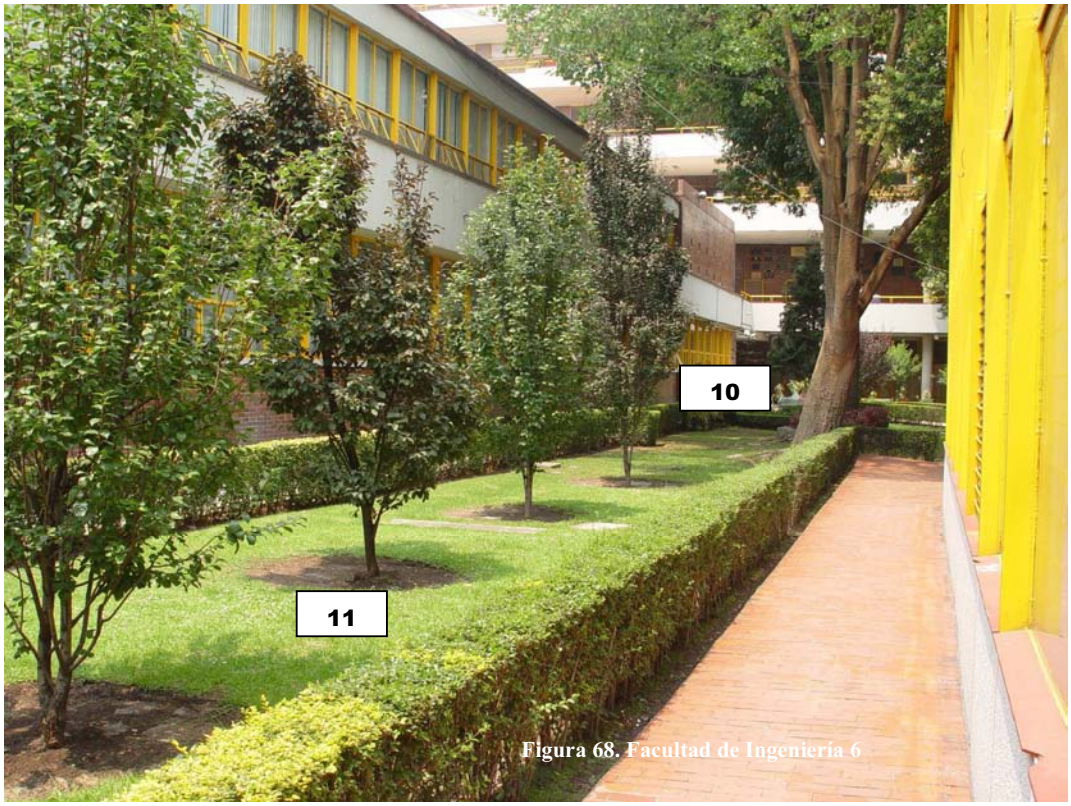


Figura 68. Facultad de Ingeniería 6

Biblioteca Enrique Rivero

Tabla 64. Facultad de Ingeniería. Biblioteca Enrique Rivero. Medición 1

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	3/5	WEP
MATERIALES3	2/5	WPA – PSK

Tabla 65. Facultad de Ingeniería. Biblioteca Enrique Rivero. Medición 2

RED	Intensidad	Seguridad
RIU	5/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	4/5	WEP
hpsetup	2/5	WEP

Tabla 66. Facultad de Ingeniería. Biblioteca Enrique Rivero. Medición 3

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	5/5	WEP
Red sin nombre	3/5	Red no segura
Hpsetup	2/5	WEP

Tabla 67. Facultad de Ingeniería. Biblioteca Enrique Rivero. Medición 4

RED	Intensidad	Seguridad
RIU	5/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)

Tsunami	5/5	WEP
MATERIALES3	1/5	WPA – PSK
Red sin nombre	4/5	Red no segura

Tabla 68. Facultad de Ingeniería. Biblioteca Enrique Rivero. Medición 5

RED	Intensidad	Seguridad
RIU	5/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	4/5	WEP
MATERIALES3	1/5	WPA – PSK
Red sin nombre	4/5	Red no segura

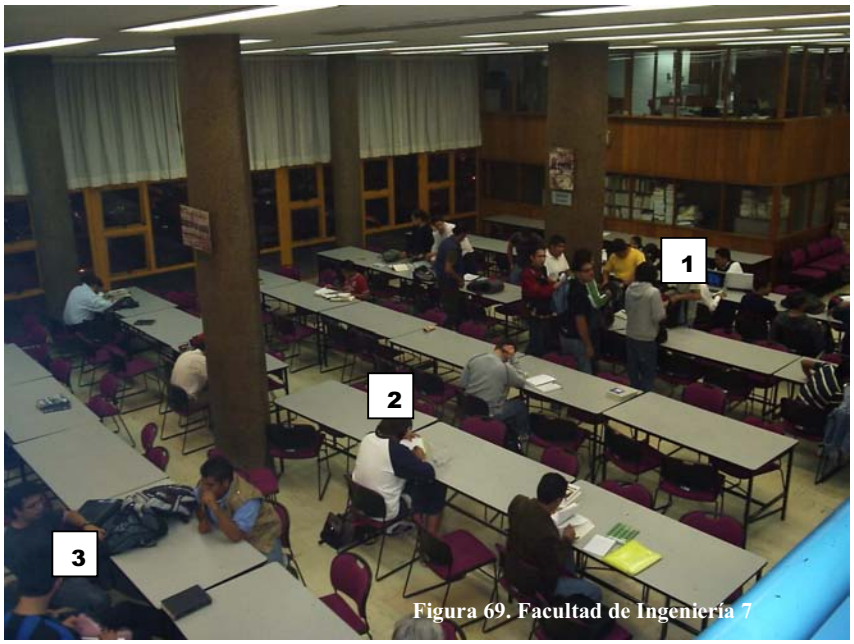


Figura 69. Facultad de Ingeniería 7

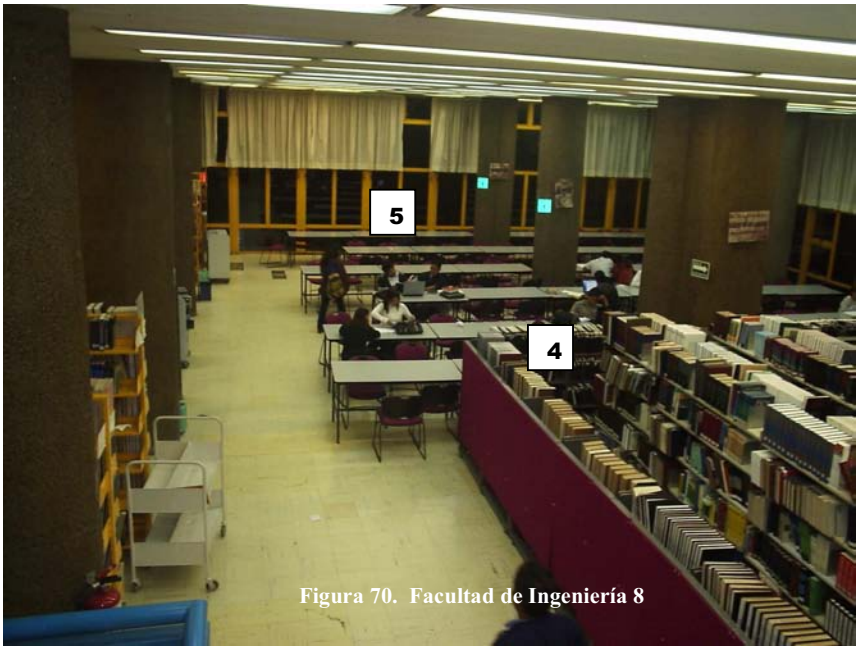


Figura 70. Facultad de Ingeniería 8

Tabla 69. Facultad de Ingeniería. Biblioteca Enrique Rivero. Parte Superior 1

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	4/5	WEP
Red sin nombre	2/5	Red no segura
Hpsetup	1/5	WEP

Tabla 70. Facultad de Ingeniería. Biblioteca Enrique Rivero. Parte Superior 2

RED	Intensidad	Seguridad
RIU	4/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	3/5	WEP
Red sin nombre	2/5	Red no segura

Tabla 71. Facultad de Ingeniería. Biblioteca Enrique Rivero. Parte Superior 3

RED	Intensidad	Seguridad
RIU	3/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	2/5	Red no segura
Hpsetup	1/5	WEP

Figura 71. Facultad de Ingeniería 9

Tabla 72. Facultad de Ingeniería. Zona de laboratorios 1

RED	Intensidad	Seguridad
RIU	2/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
Red sin nombre	1/5	Red no segura
MATERIALES3	3/5	WPA – PSK

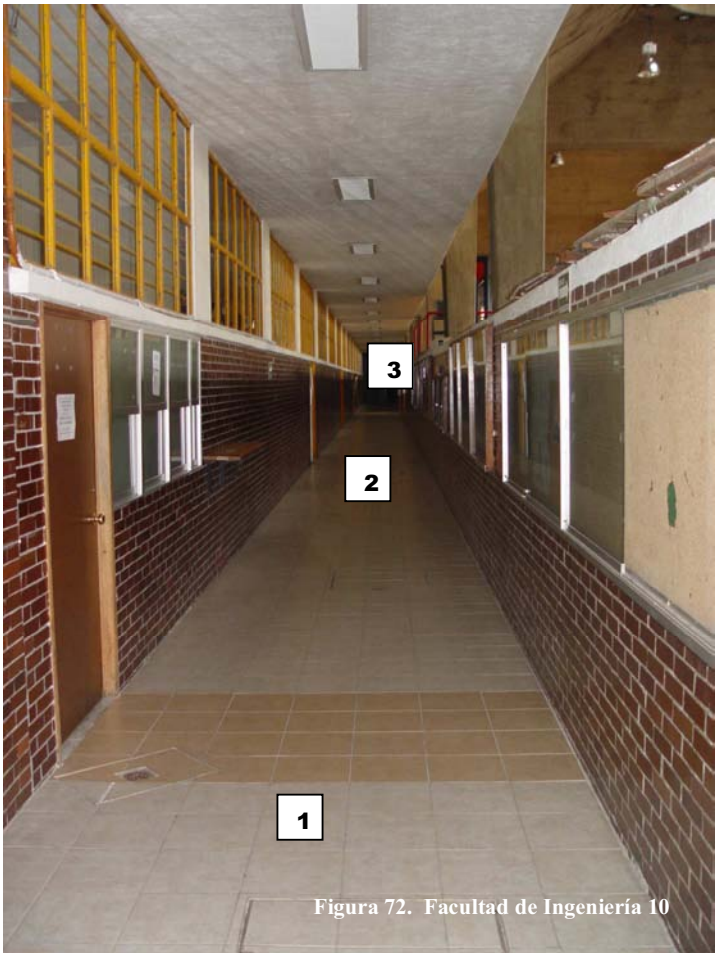


Figura 72. Facultad de Ingeniería 10

Tabla 73. Facultad de Ingeniería. Zona de laboratorios 2

RED	Intensidad	Seguridad
RIU	2/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	2/5	WEP
WIRELESS	2/5	WEP
MATERIALES3	4/5	WPA – PSK

Tabla 74. Facultad de Ingeniería. Zona de laboratorios 3

RED	Intensidad	Seguridad
WIRELESS	2/5	WEP
Tsunami	1/5	WEP
Red sin nombre	2/5	Red no segura
MATERIALES3	4/5	WPA – PSK

Tabla 75. Facultad de Ingeniería. Zona de laboratorios 4

RED	Intensidad	Seguridad
RIU	1/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	1/5	WEP
MATERIALES3	3/5	WPA – PSK

Tabla 76. Facultad de Ingeniería. Zona de laboratorios 5

RED	Intensidad	Seguridad
RIU	2/5	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	1/5	WEP
WIRELESS	1/5	WEP
MATERIALES3	3/5	WPA – PSK

Tabla 77. Facultad de Ingeniería. Zona de laboratorios 6

RED	Intensidad	Seguridad
WIRELESS	2/5	WEP
Red sin nombre	1/5	Red no segura
MATERIALES3	3/5	WPA – PSK

Ala "Poniente"

Figura 73. Facultad de Ingeniería 11

Ala "Norte"

Figura 74. Facultad de Ingeniería 12

Figura 75. Facultad de Ingeniería 13

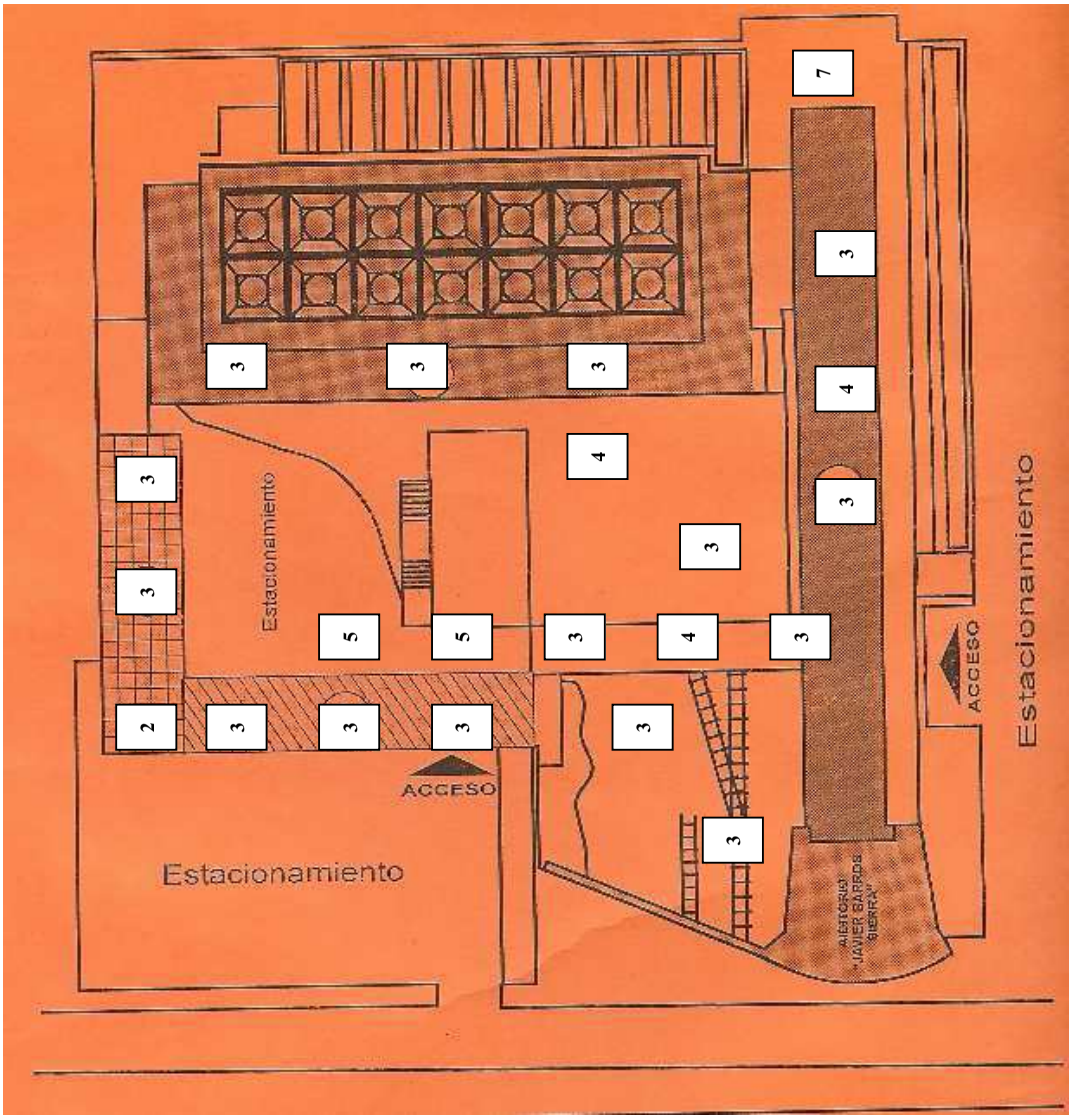


Figura 76. Cuadro resumen con el número de redes inalámbricas en la Facultad de Ingeniería

V.2 ¿Quién los administra?

Como hemos visto a través de la arquitectura y topología de la RIU, el control, administración y mantenimiento y monitoreo de la Red es de tipo centralizado, lo que permite tener los diferentes aspectos de la red bajo control.

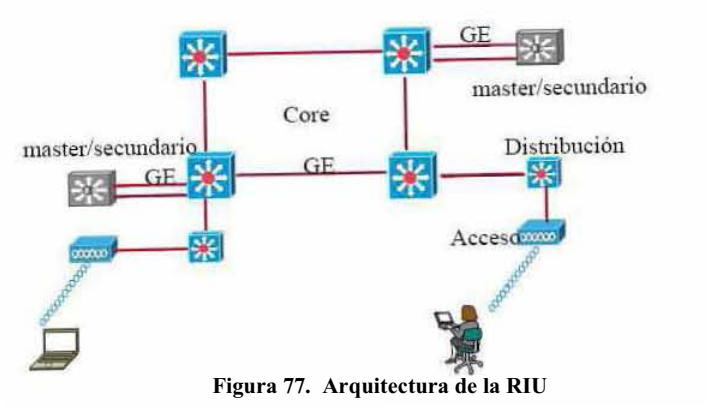


Figura 77. Arquitectura de la RIU

El departamento de la UNAM encargado de esta tarea es la Dirección General de Servicios de Cómputo Académico (DGSCA) ubicada en Ciudad Universitaria enfrente de la facultad de Contaduría y administración.

V.3 Seguridad

Esta tabla muestra la seguridad que se tiene en cada una de las redes que existen en la Facultad de Ingeniería

Tabla 78. Seguridad en la División de Ciencias Básicas

Nombre de la Red	Tipo	Seguridad
RIU	802.11 a/g	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Lab Redes	802.11 b	Red no segura
Imsa	802.11 g	WEP
Diedimei2A	802.11 a	Red no segura
LINDA WiFi	802.11 g	Red no segura
hpsetup	802.11 b	Red no segura
Mobilean	802.11 g	WEP
Diedimei2G	802.11 g	Red no segura
IVirtual	802.11 g	WEP
Red_sin_nombre	802.11 g	WEP
Red LPDI	802.11 g	WPA – PSK
Antena1	802.11 g	WEP
MEMS	802.11 b	WEP
PAEFI	802.11 g	WEP
Trino1	802.11 g	WEP
ROBOCUP	802.11 g	Red no segura
2WIREFINAL	802.11 g	WEP
LABSIMULACION	802.11 g	WPA – PSK
Lab voz	802.11 g	Red no segura
UVMU4_Biblioteca1	802.11 g	Red no segura
Mobilecam	Red ad-hoc	Red no segura
linksys	802.11 g	Red no segura

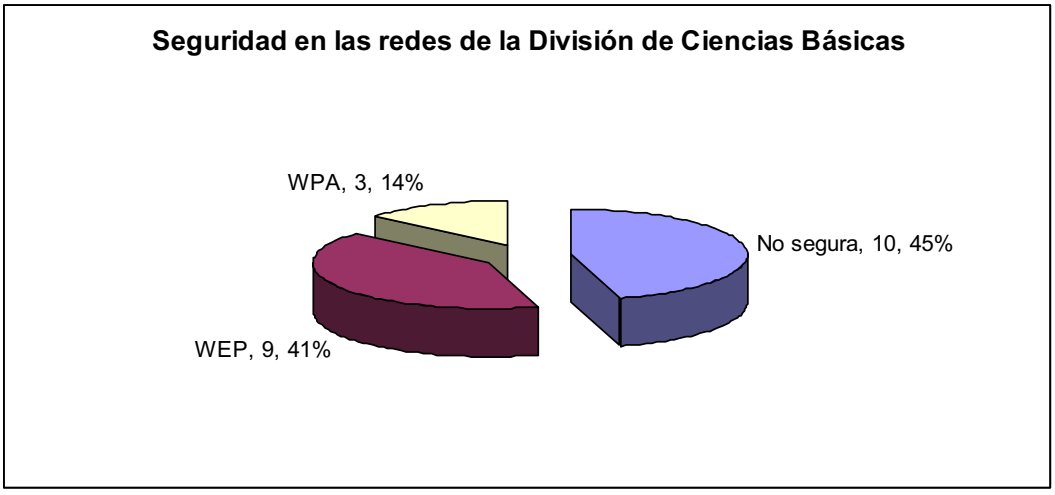
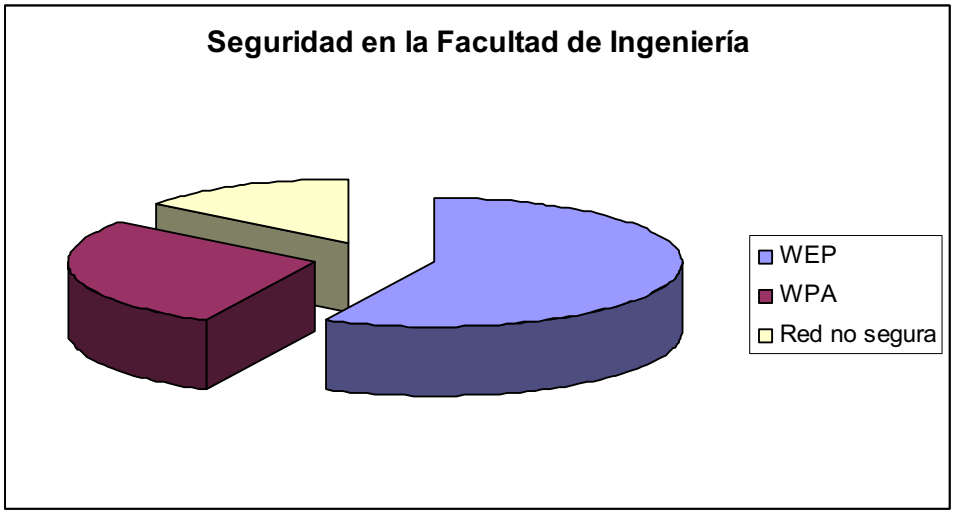


Tabla 79. Seguridad en la Facultad de Ingeniería

Nombre de la Red	Tipo	Seguridad
RIU	802.11 a/g	WPA – Enterprise Cifrado TKIP Autenticación EAP protegido (PEAP)
Tsunami	802.11 g	WEP
Red sin nombre	802.11 g	Red no segura
Hpsetup	802.11 g	WEP
riu	802.11 g	WEP
MATERIALES 3	802.11 g	WPA – PSK
WIRELESS	802.11 g	WEP



V.4 ¿Quién tiene acceso?

Usuarios Autorizados

Son usuarios autorizados los que, previa autorización y cumplimiento de los requisitos correspondientes, tienen acceso a la RIU y hacen uso de los servicios. Estos comprenden a los alumnos, académicos e investigadores de la UNAM así como estudiantes, académicos e investigadores invitados de otras instituciones.

Asignación del servicio.

Previo al cumplimiento de los requisitos que al efecto se establezcan, la DGSCA generará las cuentas de usuario para el acceso a la RIU a partir de un registro de los usuarios y distribuirá las contraseñas de manera presencial a través de la Coordinación del Centro de Atención a Usuarios, ubicada en el edificio principal de la DGSCA en el Circuito Exterior S/N.

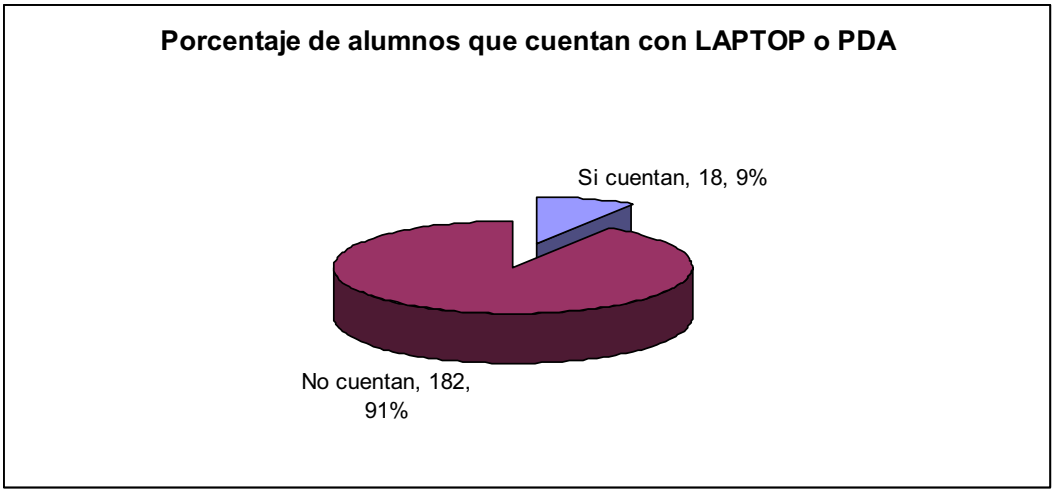
El servicio de acceso a la Red Inalámbrica será proporcionado a la comunidad estudiantil y académica universitaria en forma gratuita.

Los estudiantes usuarios de la RIU actualizarán su registro semestral o anualmente de acuerdo a sus calendarios escolares y los académicos e investigadores lo harán anualmente.

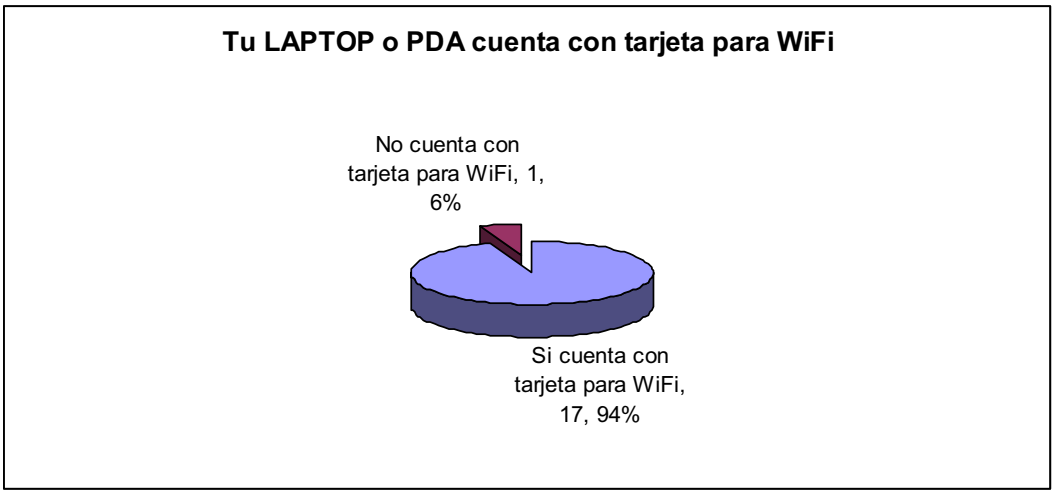
V.5 Encuesta DIE

La encuesta se llevó a cabo la semana del 26 al 30 de mayo de 2007 directamente a 200 alumnos de la facultad de ingeniería la cual mostró los siguientes resultados según las siguientes preguntas resueltas.

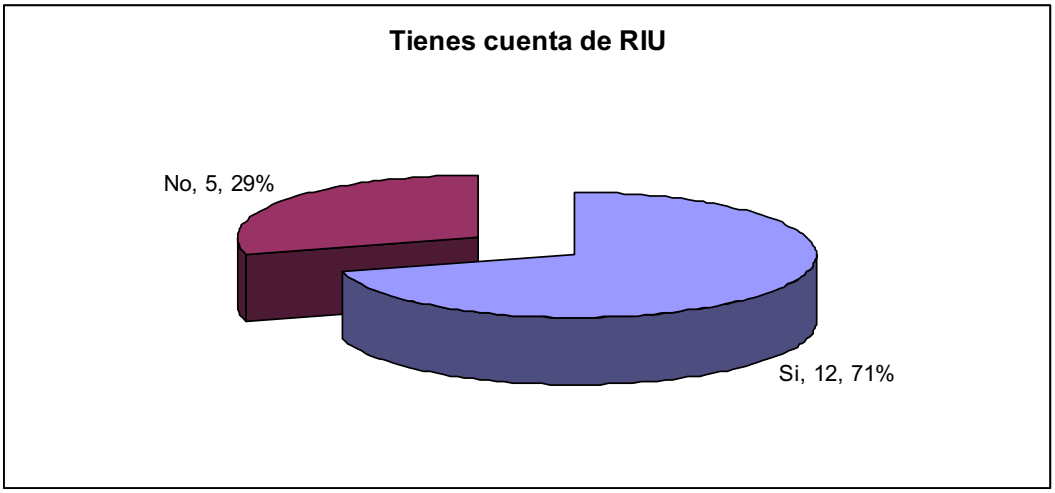
¿Tienes LAPTOP o PDA propia?



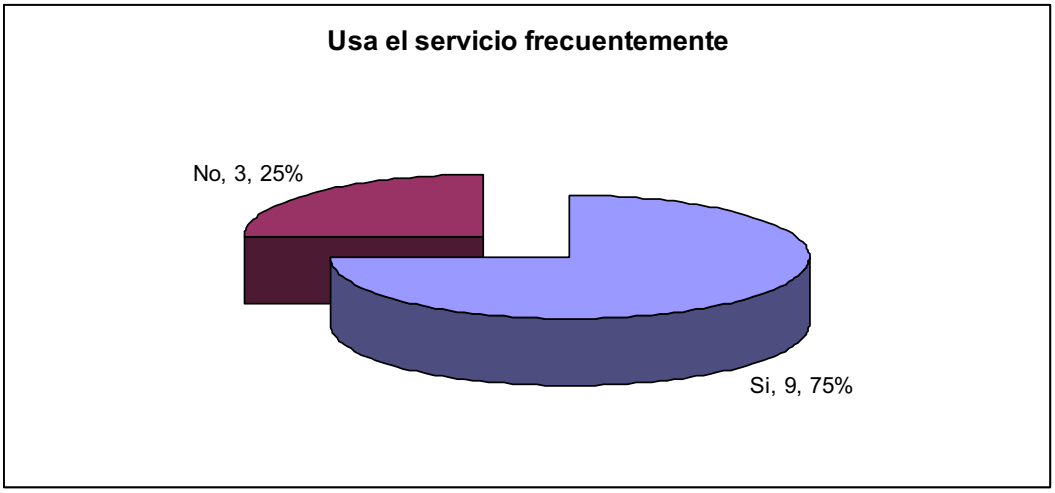
Para los alumnos que respondieron que si cuentan con LAPTOP o PDA:
¿Tu LAPTOP o PDA cuenta con tarjeta de red para WiFi?



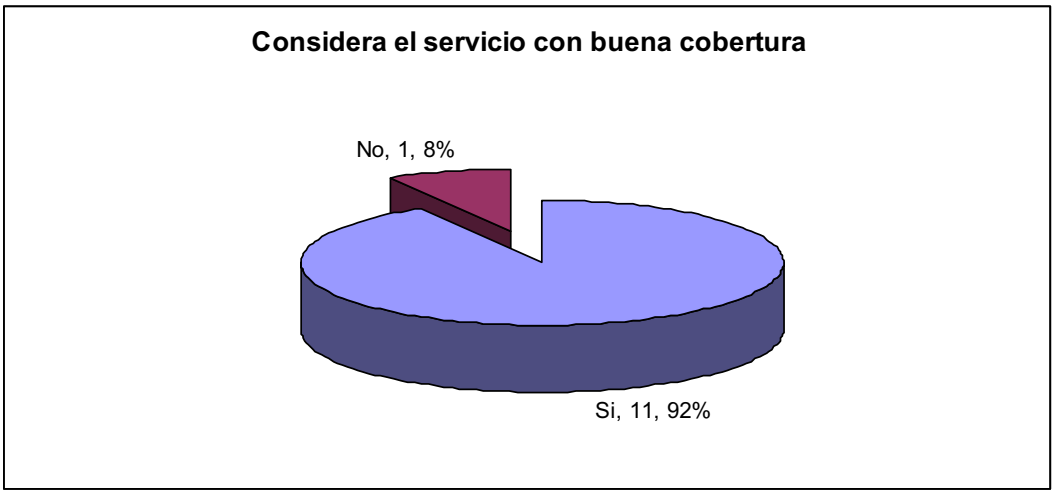
Para los alumnos que respondieron que si cuentan con tarjeta para WiFi
¿Tienes una cuenta para usar la RIU?



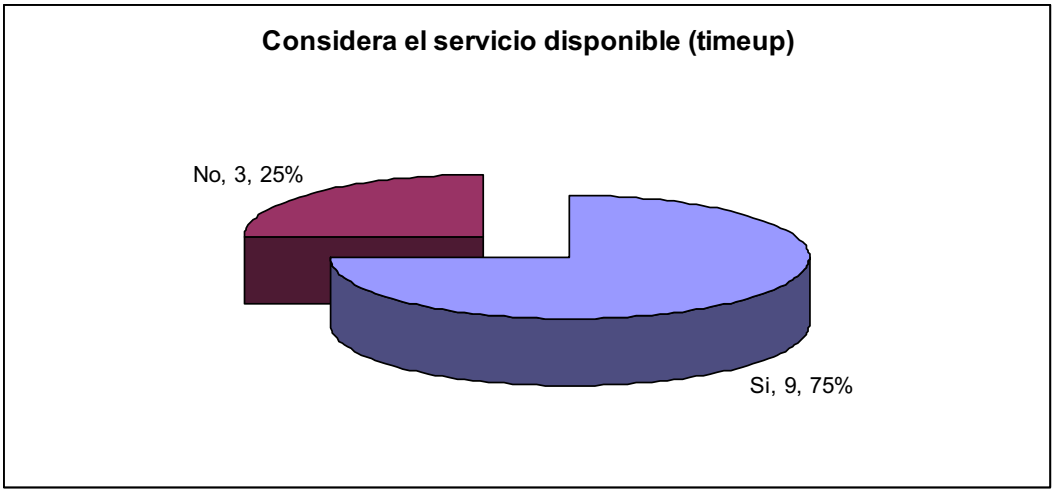
Para los alumnos que respondieron que si tienen una cuenta de RIU
¿Usas este servicio frecuentemente (mínimo una vez a la semana)?



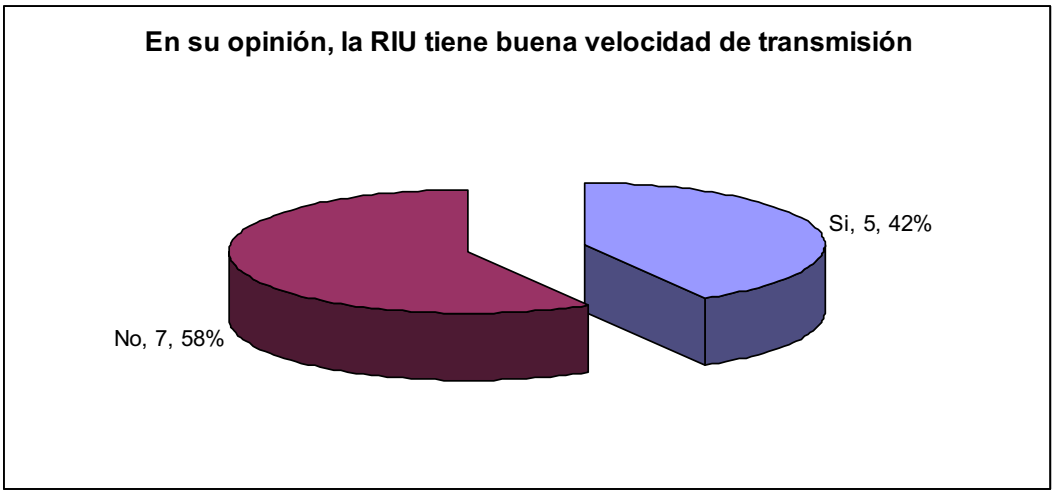
¿Consideras que el servicio es bueno en cuanto a cobertura?



¿Consideras que el servicio está disponible gran parte del tiempo?



¿Considera ud que la RIU cuenta con un buena velocidad de transmisión? (si/no)



V.5 Conclusiones

Las redes inalámbricas de área local (WLAN) cada día son más populares y han extendido su uso a diferentes campos, debido a las características particulares de la transmisión de datos.

La tecnología WLAN es flexible porque permite adaptarse a diferentes topologías y/o arquitecturas, de acuerdo a las necesidades y características del entorno de trabajo.

La banda de trabajo es de libre uso o utilización, por lo que no requiere un pago, abaratando así el costo total del uso de los equipos y tecnología, sin embargo estas tecnologías coexisten en la vida real con otras redes y puede que sí afecte su funcionamiento a causa de interferencia.

Cada día existen mayor número de fabricantes de equipos, por lo que mejores precios y mayor competencia están cada día en el mercado, lo que no quiere decir que se asegure la interoperabilidad entre estos equipos, por lo que en mi opinión las leyes deberían de asegurar que puedan ser inter-operables para beneficio de los consumidores.

En forma puntual, las ventajas y desventajas de la transmisión inalámbrica son las siguientes:

Ventajas de la transmisión inalámbrica

- Movilidad
- Ahorro de dinero y tiempo para la instalación (en comparación con una red cableada: par trenzado, cable, fibra óptica, etc.)
- Escalabilidad
- Seguridad (lugar geográfico, cobertura)

Desventajas

- Tasa de transmisión menor que una red cableada (hasta ahora)
- Seguridad (lugar geográfico)
- Cifrado de datos es requerido, así como autentificación del usuario.
- Recursos limitados (ancho de banda)
- Tasas de errores mayores
- Limitación de potencia para dispositivos inalámbricos
- Factores del medio ambiente que influyen en la transmisión
- Factores de movilidad de usuario que influyen en la transmisión (usuarios caminando, usuarios en un carro a 100km/hr)
- Las velocidades estandarizadas raramente se pueden alcanzar

En términos de velocidades, el estándar IEEE 802.11 todavía tiene un camino largo que recorrer para poder competir con las redes alámbricas, ya que solo ofrece velocidades teóricas de 1, 2, 5.5, 11 y 54 Mbps en sus distintas modalidades del estándar, sin embargo pocas veces se cumple que se pueda transmitir bajo un máximo teórico.

En términos de transmisión de frames, el IEEE 802.11 es de los más eficientes, ya que permite la fragmentación de paquetes; haciendo más eficiente el uso de ancho de banda. Además de esto ofrece otras características importantes como el uso de protocolo de supresión de colisiones, resolviendo así el problema de las terminales ocultas.

Sin embargo una de las mayores desventajas de este tipo de redes es la seguridad. El estándar por si solo ofrece políticas de seguridad muy débiles, fáciles de corromper, teniendo que implementar otros tipos de tecnologías en seguridad haciendo que la instalación sea encarecida.

La WLAN tiene como futuro la interoperabilidad con las redes celulares, esto permitirá ampliar el área de cobertura y transmisión de datos, esto permitirá la bondad de tener todos los servicios de cada una de las tecnologías que estas ofrecen haciendo su uso más flexible, barato y eficiente.

El tipo de tecnologías que hemos revisado se complementan entre sí, por lo que cubren diferentes necesidades para los consumidores y usuarios, entonces la elección de una tecnología dependerá de factores como velocidad de transmisión, número de usuarios, costo, mantenimiento, etc.

Respecto a la Facultad de Ingeniería

Las mediciones tomadas demuestran que existe una cobertura de la RIU en la mayoría de los lugares en lo que los estudiantes deben de tener el acceso, una calidad alta y un buen servicio para todos los estudiantes que lo soliciten.

Respecto a las otras redes inalámbricas nos encontramos con que muy pocas cuentan con seguridad; y las que cuentan con ella se encuentra habilitada la tecnología WEP, una muy mala elección porque muy fácilmente se puede quebrar.

El número de redes inalámbricas oscila entre las 3 y 7 dependiendo del lugar donde se mida (ver imágenes 63 y 76).

En la división de ciencias básicas el porcentaje de redes no seguras es 45% y las que cuentan con WEP 41%, mientras que en el edificio principal las no seguras son el 14% y las que cuentan con WEP el 57%.

Los alumnos que visitan la DIE con computadora son aproximadamente el 18% y un 71% de estos alumnos cuentan con una cuenta en la RIU, muchos de ellos usan el servicio frecuentemente y se tiene una buena imagen del servicio.

Se propone entonces incrementar la seguridad en las redes inalámbricas, fomentar el uso de WPA y no de WEP y así conseguir un nivel de seguridad mayor.

Bibliografía

Cisco Networking Academy Program
CCNA 1 and 2 Engineering Journal and Workbook Revised Third Edition

P. Pieda, J. Ethridge, M. Baines and F. Shallwani,
"*A Network Simulator Differentiated Services Implementation*"
Open IP, Nortel Networks
July 26, 2002.

Ing. Enrique Díaz Cerón
Apuntes del Curso Seminario de Ingeniería en Telecomunicaciones
Facultad de Ingeniería UNAM

Focus Group on Next Generation Networks
http://www.itu.int/ITU-T/ngn/fgngn/index.html

Artículo sobre redes inalámbricas WLAN por Jaime Cuellar Ruíz
http://www.enterate.unam.mx/Articulos/2004/Abril/redes.htm

Matthew Gast
802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks

The Wireless LAN Alliance
Introduction to Wireless LAN
USA 1999

Seminario AdminUNAM
Mecanismo Básico de Seguridad para Redes de Cómputo
Diciembre de 2005. DGSCA

Diferentes documentos internos de DGSCA
RIU https://www.riu.unam.mx/

Prasad, N.R.
IEEE 802.11 Aystem Design
Personal Wireless Communications, 2000 IEEE International Conference on 2000

Jorge Pérez, Juan Redondo, Vanessa Ruano
WI-FI, Análisis, diagnóstico y políticas públicas
Grupo de Análisis y prospectiva del sector de las telecomunicaciones
Noviembre 2003

Gómez Castellanos javier
Redes Inalámbricas y Móviles
2003

Balachandran, Geoffrey
Wíreless Hotspots: Current Challenges and Future Directions

Investigation of the IEEE 802.11 medium access control (MAC) Sublayer functions
Crow, B.P.

Infocom ’97. Sixteen Annual Joint Conference of the IEEE Computer and Communication Societies
Proceedings IEEE, Volume 1

Wireless Community Networks
Jain Saurabh,