UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E INSTALACIÓN DE LA RED INALÁMBRICA DEL INSTITUTO DE FÍSICA DE LA UNAM

T E S I S

QUE PARA OBTENER EL TÍTILO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

CRISTIAN MARIANO HERNÁNDEZ VEGA

DIRECTOR: L.I. NEPTALÍ GONZÁLEZ GÓMEZ

MÉXICO DISTRITO FEDERAL 2009.

Dedicatorias y Agradecimientos.

En todo este tiempo, he tenido la fortuna de contar con personas que siempre me han alentado a seguir adelante y a ser una mejor persona.

Dedicatorias:

A mis Padres, Cristina Vega y Mariano Hernández, que siempre han sido mi principal e incondicional apoyo, les debo tanto que nunca acabare de agradecer su cariño, trabajo, esfuerzos y sacrificios enfocados en el bienestar de nosotros sus hijos. Este logro es de ustedes, ¡¡¡Muchísimas Gracias!!!
¡¡¡Papá, Mamá…Los AMO!!!

A mis Hermanos, Adrian, Alán, Sharon, Natalia y Aldo, que han sido mi compañía, mi equipo, mi fuerza. Gracias por los regaños, recordatorios, cariño y confianza. Ustedes me han visto crecer y ahora yo quiero que en lo posible sigan mis pasos.
¡¡¡Los Quiero mucho hermanitos!!!

A mis abuelos Natalia Lara, Victoria Ortiz, Simón Vega (Q.E.D). Desde donde quiera que estén y Mariano Hernández, gracias por todo su cariño y por los buenos deseos de que sus nietos salieran adelante.
¡¡¡Los extraño mucho abuelitos!!!

A Dulce María Bernal Corona, que es una parte muy importante en mi vida, mi fuerza, mi inspiración, mis ganas de salir adelante, mis proyectos, mi presente y mi futuro. Gracias por tu cariño, por tu amor, por apoyarme y comprender lo importante concluir este ciclo.
¡¡¡Te Amo Dul!!!

A Familia Bernal Corona, por su apoyo, cariño y confianza, por los consejos y los ánimos, por recibirme en su casa como si fuera parte de su familia.
¡¡¡Muchas Gracias!!!

A María de los Ángeles Marmolejo, que siempre se ha interesado por mi bienestar, por el cariño que desde lejos me demuestras a mí y a toda mi familia.
¡¡Te quiero mucho madrina!!

A mis Amigos, Javier, Erick, Miguel Ángel, Franco, Alex, Tania, Melisa, Isset, Claudio, Gustavo, Daniel y Roberto, que han sido un gran apoyo y compañía en las buenas y la malas. Por las porras y ánimos, los consejos, los regaños y la confianza de que esta tesis saldría adelante.

¡¡¡Muchas Gracias!!!

Y una muy especial dedicatoria a Neptalí González Gómez, por todo el tiempo que me dedicaste, por no dejarme abandonar el proyecto, por la oportunidad que algún día me diste de aprender, no solo en lo profesional, sino también en lo personal, gracias por ser mi amigo y una excelente persona, la verdad no sé como agradecerte. A tu familia, Lilia y Montse, gracias por el apoyo y las atenciones.

No lo hubiera logrado sin tu apoyo.

¡¡¡Muchísimas Gracias Nep!!!

Y a tantos otros amigos y familiares que sería imposible mencionar, muchas gracias a todos ustedes que saben el cariño y el aprecio que les tengo, todos y cada uno de ustedes que pusieron su granito de arena para que este momento llegara.

¡¡¡Muchas!!! ¡¡¡Muchas!!! ¡¡¡Gracias!!!

Agradecimientos

A mis sinodales:

M.C. María Jaquelina López Barrientos

Ing. Noé Cruz Marín

Ing. Filiberto Manzo González

Ing. Fernando Javier Martínez Mendoza

Por el tiempo dedicado a la revisión y corrección de este trabajo de tesis, por sus observaciones y consejos.

¡¡Esta tesis es mejor gracias a ustedes!!

A la Universidad Nacional Autónoma de México, por una vida académica llena de satisfacciones.

A la Facultad de Ingeniaría, que me brindo la mejor formación que un Ingeniero puede tener.

Al Instituto de Física, que me abrió sus puertas para aprender más en el ámbito profesional y además darme la oportunidad de desarrollar mi trabajo de tesis.

Por mi raza hablará el espíritu.

Cristian Mariano Hernández Vega ..... México D.F. 2009

INTRODUCCIÓN.

El Instituto de Física cuenta con una planta académica de investigación de gran prestigio a nivel nacional e internacional, además existe un gran número estudiantes de nivel licenciatura, maestría y doctorado. Hoy día esta Institución cuenta con una infraestructura de cómputo de avanzada, que da soporte a las aplicaciones utilizadas por su planta académica, siendo esta infraestructura una herramienta fundamental para el desarrollo de las investigaciones que se realizan.

La problemática que aqueja esta institución, es la escasez del direccionamiento de IP´s y nodos de red, y la creciente demanda de servicio por parte de los usuarios, que a su vez son aumentan día con día. Actualmente el Instituto de Física cuenta con 2 segmentos de red válidos para la conexión a Internet, los cuales se encuentran saturados.

Como una alternativa a esta problemática, se propone la solución de instalar tecnologías de red del tipo WIRELESS (sin cables), que proporcionaran conectividad a la red local e Internet a los usuarios que necesiten estar conectados. Y al mismo tiempo, se evita saturar el rango de direcciones IP asignadas al IF. Las velocidades que brinda este tipo de tecnología de red (WIRELESS) son bastante aceptables comparados con las velocidades de las redes de computo tradicionales (LAN con cables). Las velocidades de conexión WIRELESS están en el rango de 11 Mbps a 54 Mbps y varían de acuerdo al radio de propagación de la señal y del estándar del hardware de los usuarios.

Por las características estructurales que tiene el Instituto de Física que son algo complicadas por los numerosos muros y su gran espesor, además de la distribución de los edificios y la geografía ya que el terreno no es uniforme está distribuido en diferentes niveles de altura. Dar esta solución representa un gran reto, además de contar con un cableado estructurado de muy buena calidad lo cual respalda nuestra solución, el diseño tiene que resolver estas limitantes con un presupuesto limitado pero suficiente para dar los mejores resultados.

En resumen, en base a los estudios y el desarrollo de esta alternativa, al final esperamos contar con la implementación de la tecnología Inalámbrica, la cual debe de ser 100% funcional y con características de seguridad y control avanzados, que garanticen la confiabilidad de las conexiones de los usuarios.

1

Marco de referencia.

1.1. Descripción del Instituto de Física de la UNAM

El Instituto de Física (IF) de la Universidad Nacional Autónoma de México, fundado en 1938, fue la primera institución dedicada a realizar investigación en Física. A lo largo de casi 7 décadas ha logrado un importante grado de madurez y desarrollo académico que lo colocan como una de las organizaciones académicas más importantes del país.

El IF se encuentra localizado en la zona de Institutos de la Ciudad Universitaria (CU). El IF tiene una amplia extensión territorial que alberga los siguientes edificios: El edificio principal, la biblioteca "Juan B. de Oyarzábal", el auditorio "Alejandra Jaidar", El edificio de los aceleradores de partículas (.7 MeVs, 2 MeVs, Peletrón y 5.5 MeVs), el edificio del taller mecánico y por último el edificio Colisur (fig. 1.1).

Fig. 1.1 Ubicación del IF de la UNAM en Ciudad Universitaria

www.google.com

Los usuarios que integran al IF se dividen en Personal Académico, Personal Administrativo y Estudiantes, los cuales hacen uso de los recursos de cómputo y de tecnologías de redes de computadoras.

El objeto de estudio de esta tesis es la elaboración del diseño e instalación de una red inalámbrica que proporcione conectividad y movilidad a todos los usuarios del IF, esta red deberá proporcionar los servicios de red que son demandados por los usuarios del IF.

1.2. Historia de las redes inalámbricas

Desde hace relativamente poco tiempo el uso de redes de computadoras y de tecnologías de información ha ido creciendo de forma vertiginosa debido al desarrollo acelerado de tecnologías de redes de computadoras.

En 1985, gracias a los cambios en las regulaciones de la Comisión Federal de Comunicaciones

(FCC: ***Federal Communications Commission***) permitieron el uso de radio a través del espectro extendido en las aplicaciones comerciales, y abrió la puerta para comercializar la tecnología.

En 1988 se introdujo en el mercado el primer sistema comercial basado en tecnología de Secuencia Directa en el Espectro Extendido (DSSS: Direct Sequence Spread Spectrum), estos sistemas operaban en una banda sin licencia y estaba en la frecuencia de los 902 y 928 MHz. Debido a que esta banda estaba ubicada cerca de la banda licenciada para los teléfonos celulares analógicos que se usaban en Norteamérica, ya que el teléfono celular estándar de la primera generación estableció un rango de frecuencias entre los 824 y los 894 MHz para las comunicaciones analógicas, se proporcionó a los fabricantes la ventaja de construir sus propios dispositivos libres de licencias con componentes existentes para los nuevos propósitos y que originalmente estaban destinados para el uso de teléfonos celulares.

En 1999, la compañía Telxon agrupo sus radios en la división de Aironet Wireless Communications, que meses más tarde fue adquirida por el gigante en la industria de redes, Cisco Systems.

La operación de la banda de los 900 MHz se proporciono para una infraestructura común en los Estados Unidos, Canadá y Australia, estaba limitada para todos los demás países. Para poder llegar a los mercados ubicados fuera de estas áreas, los fabricantes comenzaron a producir radios que operaban en la frecuencia de los 2.4 GHz del espectro que estaba disponible para la operación libre de licencia en la mayor parte de Europa y Japón.

La operación en la banda de los 2.4 GHz tuvo ventajas importantes respecto a la banda de 900 MHz. Al operar en esta banda libre, los fabricantes pudieron construir un solo radio que, mediante algunos ajustes menores, pudo venderse en todo el mundo. Con lo que proporciona mejores costos de expansión. Más aún, a medida que la operación libre de licencia fue más popular en Norteamérica, las ondas en el aire de 900MHz se saturaron no solo con equipo LAN inalámbrico sino también con los teléfonos inalámbricos que son mucho más comunes. La banda de 900 MHz comenzó a conocerse como la “banda basura”, debido a la gran cantidad de interferencia que impactaba en el desempeño y confiabilidad de las LAN inalámbricas. Sin embargo, finalmente fue el movimiento hacia la estandarización lo que selló el destino de las LAN inalámbricas en la banda de 900MHz.

1.3. 802.11: El primer estándar de LAN inalámbrica.

Al notar el beneficio común de definir estándares de la industria para las LAN (Local Area Network – Red de Área Local) inalámbricas, en 1991 diversos individuos que representaban una variedad de partes interesadas, entre los que se incluyen fabricantes competidores como Telxon, NCR, Proxim Technology y Symbol Technologies, emitieron al principio una solicitud de autorización del proyecto a la IEEE, a fin de establecer un estándar interoperable para las LAN inalámbricas. IEEE rechazo que el proyecto se llevara a cabo sobre la banda de los 900 MHz, por su carácter internacional, el estándar se inclinó por la banda de 2.4 GHz.

En 1993, los fundamentos para un estándar estaban establecidos, y en junio de 1997, el estándar 802.11 del IEEE (Institute of Electrical and Electronics Engineers), que tenía más de seis años en el proceso de creación, fue ratificado. Este primer estándar 802.11 proporcionaba velocidades de datos de 1 y 2 megabits por segundo (Mbps), una forma rudimentaria de cifrado de datos que, se puede decir, tiene un nombre confuso:Privacidad equivalente al Cableado (Wired Equivalent Privacy, WEP por sus siglas en inglés), así como la transmisión a través de las tecnologías de secuencia directa y de salto de frecuencia sobre una banda de 2.4 GHz , además de rayos infrarrojos. Los aspectos relacionados con los rayos infrarrojos de este estándar obtuvieron un pequeño impulso comercial y hoy día representan sólo una pequeña parte de la historia del estándar.

1.4. Definición de las redes inalámbricas

Se llama comunicación inalámbrica a aquella que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación con teléfono móvil es inalámbrica, mientras que una comunicación con teléfono tradicional no lo es.

Basándonos en conceptos de varios autores, podemos definir a una red inalámbrica de la siguiente manera:

Red inalámbrica: “Una red inalámbrica posibilita la comunicación de dos o más dispositivos sin el empleo de cables”, en la cual los medios de comunicación entre sus componentes son ondas electromagnéticas. Se utilizan ondas de radio de bajo poder que normalmente no tienen regulación. La transmisión y la recepción se realizan a través de antenas.

Los usos más comunes para conectar aparatos de alta tecnología, se incluyen:

- IrDA (Infra red Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo.

- Bluetooth es una de las tecnologías de redes inalámbricas de área personal más conocidas, al contrario que otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para redes de computadoras, sino más bien, para comunicar una computadora o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular o manos libres, un PDA con su Computadora, o la misma computadora con una impresora, etc.

- Wi-Fi (Wireless Fidelity, "Fidelidad inalámbrica") es el sistema normalizado por la IEEE y que en realidad nos referimos al 802.11b, y se pueden establecer comunicaciones a una velocidad de 11 Mbps, alcanzándose en teoría distancias de hasta varios cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta 108 Mbps (Mega bits por segundo).

1.5. Evolución de las redes inalámbricas

Los expertos empezaban a investigar en las redes inalámbricas hace ya más de 30 años. Los primeros experimentos fueron de la mano de uno de los grandes gigantes en la historia de la informática, IBM (International Busness Machines).

En 1979 IBM publicaba los resultados de su experimento con infrarrojos en una fábrica suiza. La idea de los ingenieros era construir una red local en la fábrica. Los resultados se publicaron en el volumen 67 de procedimientos del IEEE y han sido considerados como el punto de partida en la línea evolutiva de las redes inalámbricas.

Las siguientes investigaciones se harían en laboratorios, siempre utilizando altas frecuencias, hasta que en 1985 la FCC (Federal Communication Comission – Comisión Federal de Comunicaciones) asigna una serie de bandas al uso de IMS (Industrial, Scientific and Medical). La FCC es la agencia federal de EEUU encargada de regular y administrar en telecomunicaciones.

Esta asignación se tradujo a una mayor actividad en la industria y la investigación de WLAN (red inalámbrica de área local) empezaba a enfocarse al mercado. Seis años más tarde, en 1991, se publicaban los primeros trabajos de WLAN propiamente dicha, ya que según la norma IEEE 802 solo se considera WLAN a aquellas redes que transmitan al menos a 1 Mbps.

La red inalámbrica de alcance local ya existía pero su introducción en el mercado e implantación a nivel doméstico y laboral aun tendría que esperar unos años. Uno de los factores que supuso un gran empuje al desarrollo de este tipo de red fue el auge de Laptops y PDA en el mercado, ya que este tipo de producto portátil reclamaba más la necesidad de una red sin ataduras, sin cables.

1.6. La creación del estándar Wi-Fi.

Cualquier red inalámbrica se basa en la transmisión de datos mediante ondas electromagnéticas, según la capacidad de la red y del tipo de onda utilizada hablamos de una u otra red inalámbrica.

Wi-Fi es una de ellas, en este caso el alcance de la red es bastante limitado por lo que se utiliza a nivel doméstico y oficina. Por eso mismo es la más popular ya que muchos usuarios se han decidido por eliminar los cables que le permiten la conexión a Internet, de manera que es posible conectarse a la red desde cualquier lugar de la casa.

Los inicios de cualquier descubrimiento suelen ser difíciles y uno de los principales problemas a los que se enfrenta es el establecimiento de un estándar. Por ello los principales fabricantes de redes inalámbricas decidieron asociarse para definir los estándares y facilitar la integración en el mercado de las redes inalámbricas.

Nokia, 3com, Airones, Intersil, Lucent Technologies y Symbol Technologies eran los principales vendedores de soluciones inalámbricas en los años 90. En 1999 se asociaron bajo el nombre de WECA (Wireless Ethernet Compability Alliance - Alianza de Compatibilidad Ethernet Inalámbrica). Desde el 2003 el nombre de esta asociación es Wí-Fi Alliance y ahora comprende más de 150 empresas.

Wí-Fi Alliance se encarga de adoptar, probar y certificar que los equipos cumplen con los estándares que han fijado. Su objetivo siempre ha sido crear una marca que fomente la tecnología inalámbrica y que asegure la compatibilidad e interoperabilidad entre equipos.

WIMAX

Como parte de la familia de estándares IEE 802, existe uno que está dedicado a las tecnologías inalámbricas con mayor cobertura, este es el IEEE 802.16 o WIMAX.

WIMAX son las siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas). Es una norma de transmisión de datos usando ondas de radio.

WiMAX está pensado principalmente como tecnología de "última milla" y se puede usar para enlaces de acceso, MAN o incluso WAN. Destaca WiMAX por su capacidad como tecnología portadora, sobre la que se puede transportar IP, TDM, T1/E1, ATM, Frame Relay y voz, lo que la hace perfectamente adecuada para entornos de grandes redes corporativas de voz y datos así como para operadores de telecomunicaciones que se vean obligadas a usar enlaces inalámbricos como parte de su Backbone. Para cumplir este último requisito era imprescindible contar con diferentes niveles de calidad de servicio así como el uso de diferentes canales de comunicación en un mismo radio enlace físico. Asimismo permite cubrir distancias bastante respetables sin línea de vista directa (N-LOS).

Para garantizar la interoperabilidad entre los distintos fabricantes, resulta necesario que los equipos cuenten con el distintivo WiMAX Forum, ya que la mayoría del equipamiento que se puede encontrar en el mercado, es de tipo propietario.

La incorporación chipset con soporte 802.16d y 802.16e, en los Notebook, facilitara que esta tecnología se desarrolle y pueda llegar al usuario convirtiéndose en un interface habitual.

La existencia de tecnología WiMAX, incorporada los Notebook, permitirá a los operadores que apuesten por WiMAX en las bandas licenciadas, amortizar sus inversiones, teniendo a acceso a un mercado de usuarios dotados de equipos portátiles.

Dentro de la familia de los sistemas de radio en bandas libres (Wi-Fi), también podemos encontrar equipamiento orientado a la creación de enlaces punto a punto ó punto multipunto, también existen los sistemas llamados "WiMAX sin licencia" que suelen trabajar en bandas 2,4Ghz y 5,4Ghz, este equipamiento suele ser Wi-Fi 802.11a, en muchas ocasiones, pero está dotado de antenas direccionales para facilitar un mayor alcance.

Para el establecimiento de las WirelessMAN (802.16), resulta conveniente contar con reservas de espectro radioeléctrico, ya que garantiza la carencia de interferencias.

Características de WIMAX

- Capa MAC con soporte de múltiples especificaciones físicas.
- Distancias de hasta 50 kilómetros.
- Velocidades de hasta 70 Mbps.
- Facilidades para añadir más canales.
- Anchos de banda configurables y no cerrados.

Evolución de WIMAX.

802.16: Utiliza espectro licenciado en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbps en celdas de 3 a 8 kilómetros. Soporta calidad de servicio. Publicado en 2002.

802.16 a: Ampliación del estándar 802.16 hacia bandas de 2 a 11 GHz, con sistemas NLOS (Non Line Of Site, Sin Línea de Vista) y LOS, y protocolo PTP y PTMP. Publicado en abril de 2003

802.16 c: Ampliación del estándar 802.16 para definir las características y especificaciones en la banda d: 10-66 GHz. Publicado en enero de 2003

802.16 d: Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16-2004 en junio de 2004 (La última versión del estándar)

802.16 e: Extensión del 802.16 que incluye la conexión de banda ancha nómada para elementos portátiles del estilo a Notebooks. Publicado en diciembre de 2005.

2

Metodología de solución del Problema.

Un procedimiento general para resolver problemas de ingeniería se puede resumir en cinco pasos, los cuales son:

- *Formulación o planteamiento del problema*: el problema del que se trate se define en forma amplia y sin detalle.
- *Análisis del problema*: en esta etapa se define con todo detalle.
- *Búsqueda de soluciones*: las soluciones alternativas se reúnen mediante indagación, invención, investigación, etc.
- *Decisión*: todas las alternativas se evalúan, comparan y seleccionan hasta que se obtiene la solución óptima.
- *Especificación*: la solución elegida se expone por escrito detalladamente.

A este procedimiento se le conoce como “proceso de diseño”.

Este proceso de diseño abarca las actividades y eventos que transcurren entre el reconocimiento de un problema y la especificación de la solución del mismo sea funcional, económica y satisfactoria de algún modo. El diseño es el proceso general mediante el cual, como ingenieros

aplicamos nuestros conocimientos, aptitudes y puntos de vista a la solución de un problema o satisfacción de una necesidad.

Nuestra base de conocimientos tanto académicos, empíricos y científicos, así como trabajos de investigación, artículos y bibliografía relacionada con el tema, nos ayudara a resolver la problemática que nos presenta el Instituto de Física de la UNAM en cuanto a demanda de servicios de red. ya que existen variables controladas como capacidades de los equipos, teoría de cableado estructurado y conocimientos documentados de el uso de equipos y frecuencias para transmisión de datos, así como variables desconocidas como el comportamiento de estos mismos equipos dentro de la arquitectura y geografía del Instituto de Física. Esto con el fin de obtener alguna solución flexible que no dependa de un solo método o situación, ya que en caso necesario se puede recurrir al "error o acierto" y al final poder hacer un análisis de los resultados y confirmar que nuestra hipótesis llega a buen término.

2.1. Planteamiento del problema

El Instituto de Física cuenta con una infraestructura de cómputo de avanzada, que da soporte a las aplicaciones utilizadas por su comunidad académica, siendo esta infraestructura una herramienta fundamental para el desarrollo de las investigaciones que ahí se realizan.

La problemática que aqueja esta institución, es la escasez del direccionamiento de IP´s y nodos de red, actualmente cuenta con 2 segmentos de red homologados para la conexión a Internet, los cuales están saturados.

Para dar solución a esta problemática se propone implementar una red inalámbrica (WIRELESS), la cual nos brinda velocidades que son bastante aceptables comparados con las velocidades de las redes de computo tradicionales (LAN con cables). Las velocidades de conexión WIRELESS están en el rango de 11 Mbps a 54 Mbps y varían de acuerdo al radio de propagación de la señal y del estándar del hardware de los usuarios.

En resumen, con el desarrollo de la red inalámbrica se intenta cubrir las siguientes limitantes:

- Los equipos de red (switches) no cuentan con la densidad de puertos que demandan los usuarios.
- La escases de direcciones IP (Internet Protocol) homologadas.
- No se cuenta con los recursos financieros suficientes para la instalación de cableado estructurado de un mayor número de nodos de red, y para la adquisición de switches de red con mayor densidad de puertos.

3

Marco teórico.

Para el desarrollo de la red inalámbrica se tomaron en cuenta los conceptos básicos y complementarios que se abordan a lo largo de este capítulo. El fin de este capítulo es documentar el tipo de conocimientos e información necesarios poder realizar un proyecto de este tipo, además del IFUNAM, podamos realizarlo en cualquier otro tipo de instalación y obtener resultados óptimos.

3.1 Redes de Área Local

Introducción a las Redes de Área Local

Una red de área local es la interconexión de dispositivos de cómputo que pueden comunicarse entre sí y compartir recursos comunes.

Las primeras redes que se instalaron en algunas compañías, incluyendo IBM, Honeywell y DEC (Digital Equipment Corporation) tenían sus propios estándares que definían la forma en que se debían conectar las computadoras y recursos entre si. Estos estándares establecían los mecanismos para poder transmitir información de una computadora a otra, y no fueron totalmente compatibles entre ellos.

Posteriormente, las organizaciones dedicadas a la creación de estándares, incluyendo la ISO (Organización de Estándares Internacionales) y el IEEE (Instituto de Ingenieros Eléctricos y

Electrónicos), desarrollaron modelos para el diseño de cualquier red de computadoras que fueron reconocidos y aceptados internacionalmente como estándares.

3.2. Red de Área Local (LAN)

Una red de área local es la interconexión de computadoras y periféricos para compartir recursos en común (discos, impresoras, programas, etc.). Su extensión está limitada físicamente a un edificio o a una distancia de unos cuantos kilómetros. (Figura 3-1)

El término red de área local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos

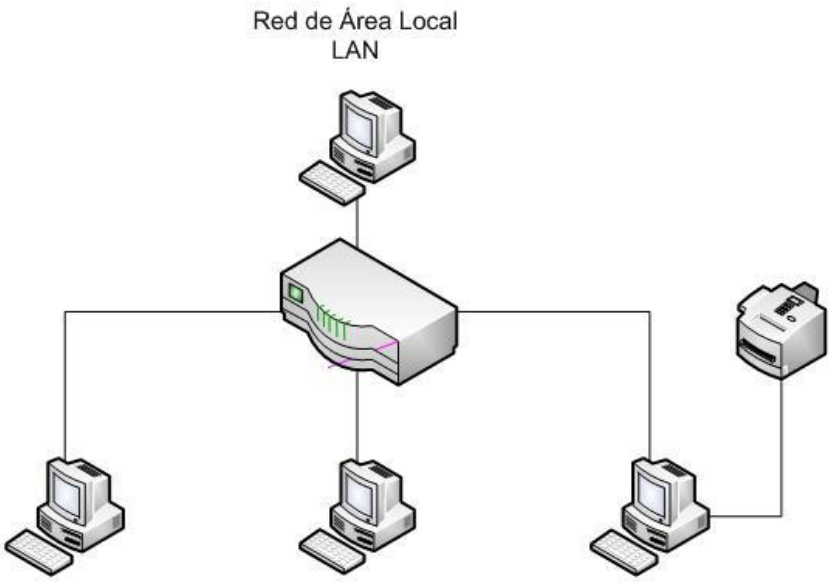


Figura 3-1 Red de Área Local.

3.3. Estándares de las Redes de Área Local

Los estándares definen la forma de conectar componentes de hardware en las redes y los protocolos (o reglas) de uso cuando se establecen comunicaciones por red. Los beneficios de la estandarización se ven reflejados en la reducción de los costos de los equipos, la facilidad de conectar dispositivos de diferentes tipos y marcas. Los estándares más populares son: ARCnet, Ethernet y TokenRing. Hoy día Ethernet ha evolucionado en sus capacidades y es el más usado para Redes de Área Local.

3.4. Modelo OSI

Fue creada por la ISO (Organización Internacional de Normas) ya que había la necesidad de tener un mejor control del manejo de las comunicaciones y poder trabajar con equipos heterogéneos sin que exista problema alguno, consiste en una división de 7 capas (Figura 3-2) y cada una de ellas tiene asignadas tareas; es decir, fue creado para tener un modelo de referencia para la normalización de sistemas abiertos.

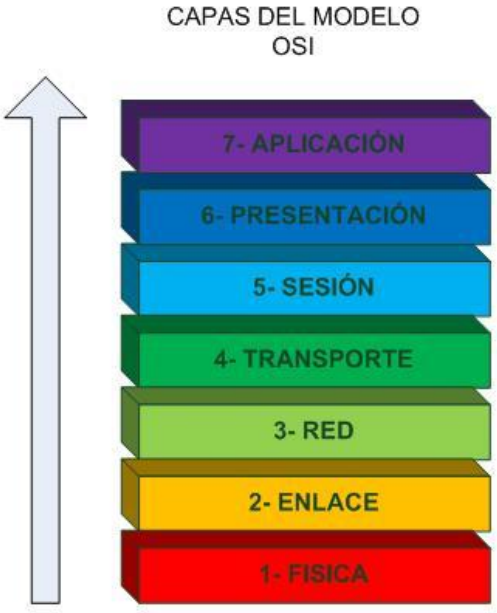


Figura 3-2 Modelo OSI

3.4.1. Aplicación del Modelo OSI

El propósito del modelo OSI es segmentar las diversas funciones que se requieren para transportar la información cuando dos computadoras se comunican.

El objetivo de cada nivel es proporcionar los servicios necesarios para el nivel superior inmediato, cada nivel se comunica con sus niveles adyacentes en una computadora. La interacción entre los niveles adyacentes se llama interfaz. La interfaz define que servicios ofrecen los niveles inferiores de redes a los niveles superiores, y la forma en que estos servicios serán accedidos. El conjunto de normas usadas para comunicarse entre los niveles se llama protocolo.

3.4.2. Capas o niveles del Modelo OSI

Nivel Físico

Esta capa se encarga de la transferencia de información mediante bits por medio del canal de comunicación, donde por cada bit enviado se debe recibir el mismo. Toma en cuenta tanto los aspectos mecánicos, eléctricos y el medio de transmisión físico. En esta capa se asignan los niveles de voltaje, y se define si la comunicación es en serie o paralela, full duplex o half duplex, reglas para iniciar y establecer o terminar la comunicación. Este nivel está relacionado únicamente al hardware.

Nivel de datos

Esta capa tiene a su cargo formar las tramas de los datos a transmitir, empaquetarlos y al mismo tiempo detectar y corregir los errores que se presenten en dicha transmisión así como la sincronización de la información.

Nivel de Red

Esta capa se ocupa de enviar la información a su destino escogiendo la mejor ruta; es la encargada de evitar un congestionamiento de información además de ser la responsable de que redes heterogéneas puedan interconectarse.

Nivel de Transporte

Provee un mecanismo de intercambio de información muy confiable entre las computadoras, debido a que es el responsable del manejo, la detección y corrección de errores. En este nivel se establecen, mantienen y terminan las conexiones lógicas para la transferencia de información.

Nivel de Sesión

Este nivel permite que dos aplicaciones en diferentes computadoras establezcan, usen y finalicen la conexión llamada sesión. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas. En este nivel se administra el control del diálogo. Si la comunicación falla y es detectado, el nivel de sesión puede retransmitir la información para completar el proceso en la comunicación.

Nivel de Presentación

Este nivel traduce o transfiere la información para ser visualizada es aquí donde se da la codificación y decodificación, comprensión y descompresión, el cifrado y descifrado. Define el formato en que la información será presentada al usuario e intercambiada entre ellos.

Nivel de Aplicación

Este nivel representa el servicio que soporta directamente las aplicaciones de los usuarios. Entre estas aplicaciones se encuentran la transferencia de archivos (FTP), acceso a bases de datos y correo electrónico.

3.5. Modelo IEEE 802

El Instituto de Ingeniero Eléctricos y Electrónicos es una de las organizaciones que establecen estándares para diversas áreas técnicas. El proyecto para la estandarización de las redes de área local (LAN), el cual se denominó 802, debido al año y mes en que fue puesto en operación (febrero de 1980).

Este modelo 802 definió los estándares de las redes para los niveles físico y de datos del modelo OSI. En este modelo diferentes métodos de acceso están a cargo de varios grupos de trabajo. La siguiente lista contiene los estándares de los diferentes grupos de trabajo del proyecto 802.

802.1	Nivel MAC de puentes (bridges) y su administración
802.2	Control de enlace lógico
802.3	CSMA/CD (Ethernet) 10Base-5 10Base-2 10BASE-T 1000BASE-X Gbit/s Ethernet sobre Fibra Optica 1000BASE-T Gbit/s Ethernet sobre Par Trenzado Fast Ethernet a 100 Mbit/s 100BASE-TX 100BASE-T4 100BASE-FX
802.4	Token Bus*
802.5	Token Ring
802.6	Red de área metropolitana *
802.7	Grupo de Asesoría Técnica sobre banda ancha*
802.8	Grupo de Asesoría Técnica sobre fibra óptica*

802.9	Red de Área Local de servicios integrados*
802.10	Seguridad interoperable en Redes de Área Local*
802.11	Red local inalámbrica, también conocido como Wi-Fi
802.12	Prioridad de demanda
802.13	(no usado)
802.14	Cable módems, es decir módems para televisión por cable*
802.15	Red de área personal inalámbrica
802.16	Acceso inalámbrico de Banda Ancha para acceso inalámbrico desde casa.
802.17	Anillos de paquetes con recuperación, se supone que esto es aplicable a cualquier tamaño de red, y está bastante orientado a anillos de fibra óptica
802.18	Grupo de Asesoría Técnica sobre Normativas de Radio
802.19	Grupo de Asesoría Técnica sobre Coexistencia.
802.20	Acceso inalámbrico de Banda ancha móvil, es muy similar al 802.16, pero en movimiento
802.21	Interoperabilidad independiente del medio
802.22	Red inalámbrica de área regional.

Tabla 3-1 – Estándares de la IEEE 802 (*abandonados)

3.6. Topologías de la Redes de Área Local

En el nivel físico, cada red de área local tiene definido sus propias características. La forma en que se conectan las computadoras en una red se llama topología. Existe la topología en bus, en estrella, en anillo; y para redes complejas, topologías mixtas o hibridas, dependiendo de la complejidad del diseño.

3.6.1. Tipos de Conexión

El tipo de conexión hace referencia a las diferentes formas en las que se pueden interconectar los equipos que están dentro de una red o que la conforman.

Existen dos tipos de conexión a una red: la conexión punto a punto y la conexión multipunto.

Punto a punto: Es una conexión entre dos dispositivos mediante un cable.

Multipunto: Es una conexión que usa un solo cable para conectar más de dos dispositivos.

3.6.2. Topología en BUS

Esta topología consiste en que todas las computadoras están conectadas a un mismo cable y cada computadora representa un nodo, cuando 2 o más máquinas quieren enviar información se puede crear una colisión por eso se debe contar con un mecanismo que se encargue de resolver dicho conflicto (CSMA/CD – Carrier Sense Media Access / Collision Detect). Los tipos de cable usados en está topología son: el cable coaxial grueso (hasta 500 mts de longitud) y cable coaxial delgado (hasta 185 mts de longitud). (Figura 3-3)

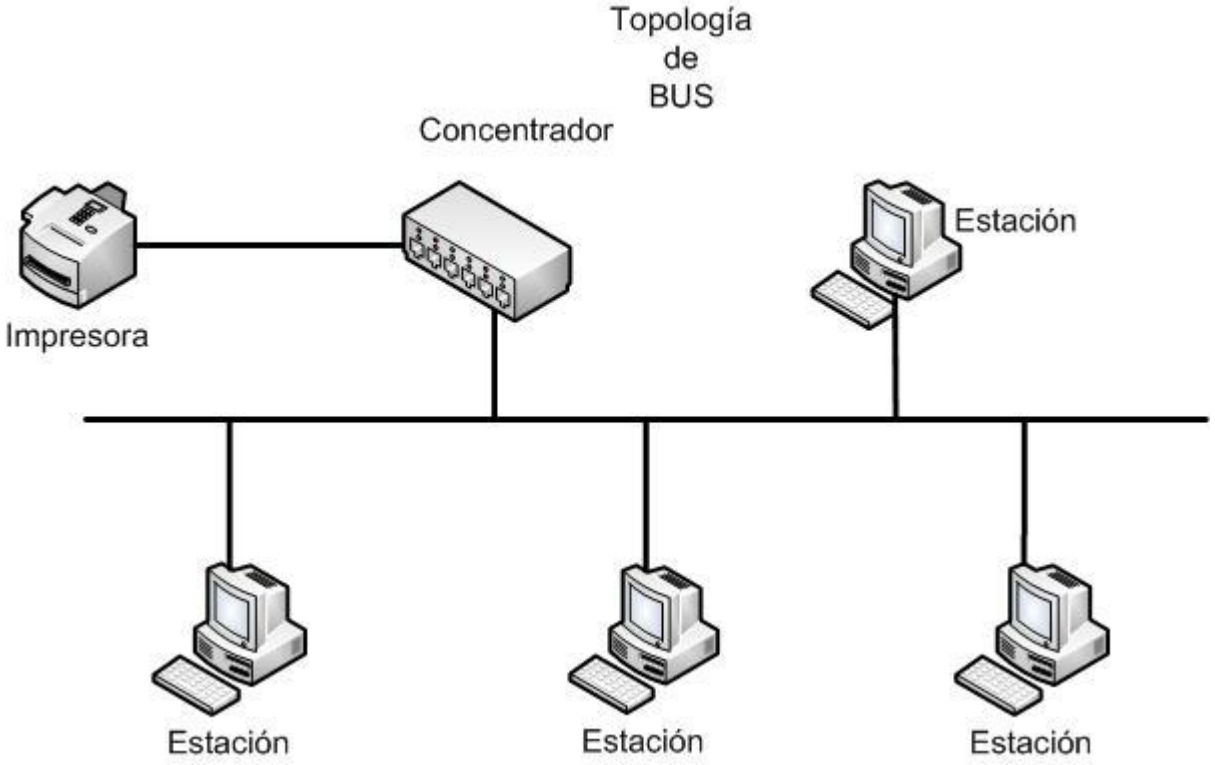


Figura 3-3 Topología tipo BUS

3.6.3. Topología en Anillo

La topología en anillo es una red punto a punto donde los dispositivos se conectan a un concentrador que es el encargado de formar eléctricamente el anillo, el mensaje viaja en una sola dirección predeterminada, el dispositivo que recibe el mensaje tiene la facultad de reenviarlo si dicho dispositivo no es el destino final. (Figura 3-4)

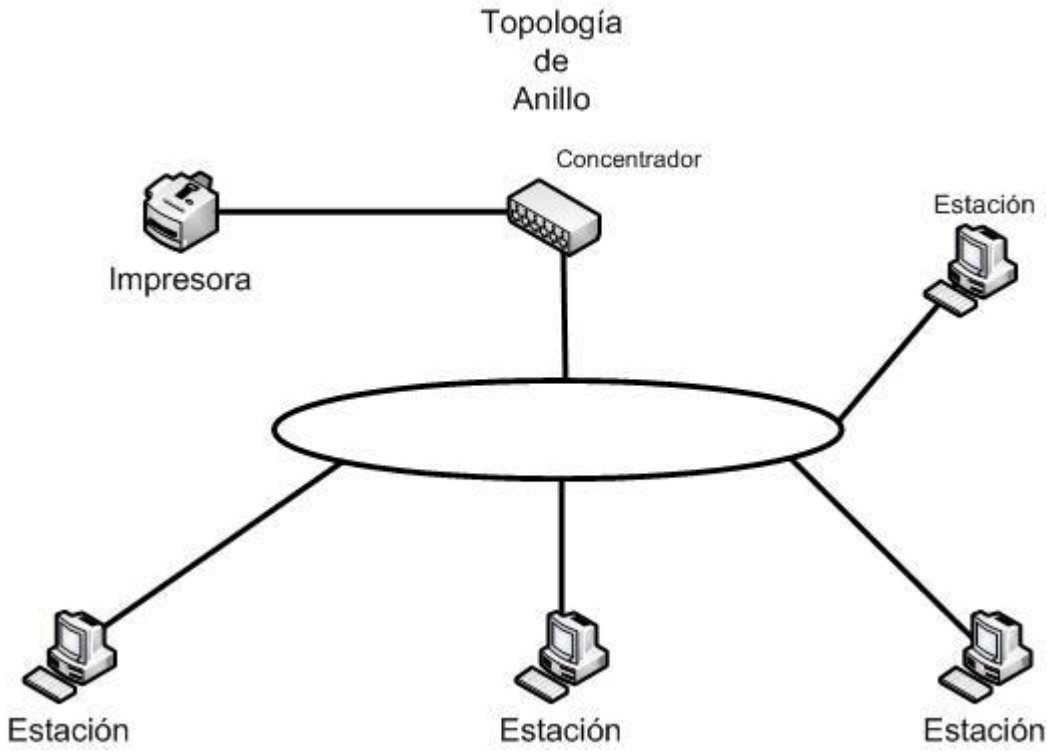


Figura 3-4: Topología de Anillo.

3.6.4. Topología en Estrella

Es una topología de red punto a punto, consiste en conectar cada computadora a un equipo central (concentrador). Cada dispositivo se conecta por un cable separado a través del concentrador. Internamente el concentrador maneja una topología tipo bus. (Figura 3-5)

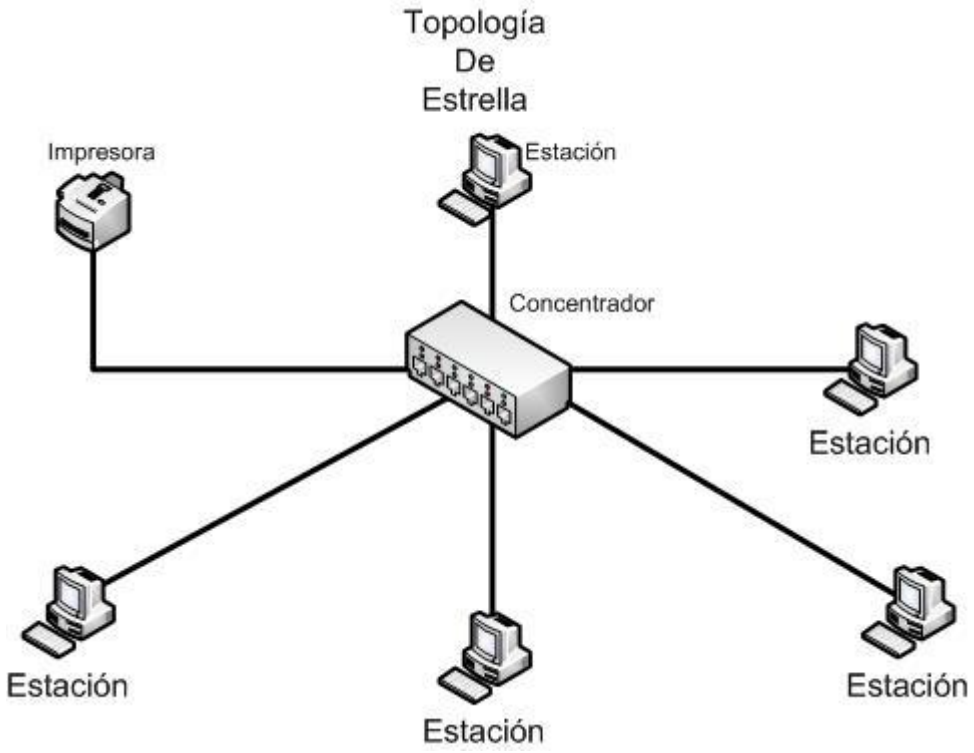


Figura 3-5: Topología de Estrella

3.6.5. Tipos de Acceso

Las topologías en estrella y anillo físicamente tienen forma de estrella, pero dependiendo del concentrador que se utilicé permanecen con esta forma física o se genera un anillo. En este caso hay dos formas de comunicar los dispositivos con el concentrador de la topología, estos son: poleo y contención.

Tipo de acceso de poleo: existe una estación encargada de asignar los permisos a cada dispositivo dentro de la red para enviar su información, si este dispositivo tiene permiso, éste comienza su transferencia a su destinatario, si no debe esperar su turno.

Tipo de acceso de contención: cada dispositivo transmite en la red sólo cuando nadie está enviando información, y el concentrador se encarga de administrar el tráfico. Este tipo de acceso permite un mayor número de paquetes y mejor rendimiento de la red.

3.6.6. Topología Hibrida

La topología hibrida es un conjunto de todas las anteriores. Generalmente se usa cuando el diseño de la red es complejo, o existe un gran número de dispositivos en la red que obliga a configurar una red con este tipo de topología. (Figura 3-6)

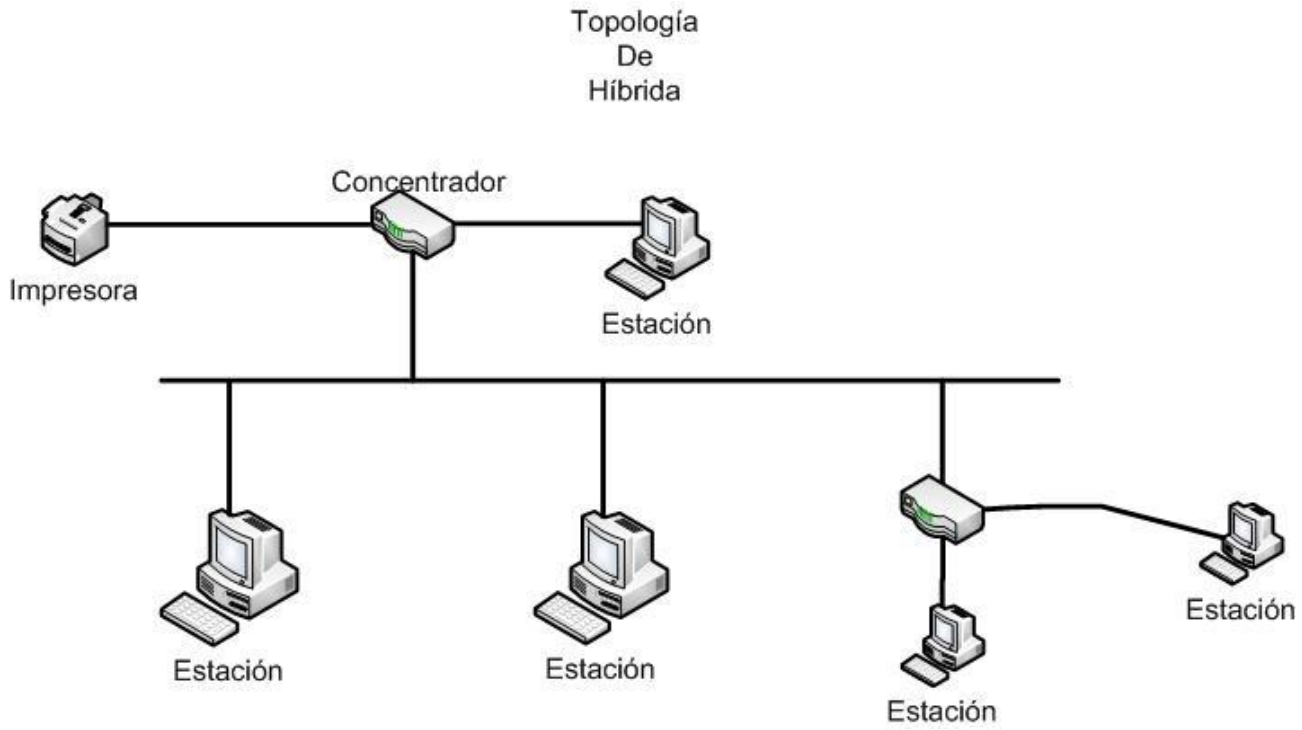


Figura 3-6: Topología Hibrida

3.6.7. Tipos de Medios

El medio de transmisión se usa para transportar las señales de la red de un dispositivo a otro.

Las redes de área local pueden interconectarse usando diferentes tipos de medios, principalmente se usan tres tipos de medios físicos: coaxial, par trenzado (UTP Unshielded Twisted Pair) y fibra óptica. La capacidad de transmisión que soporta cada tipo de medio se mide en millones de bits por segundo o Mbps.

Cableado estructurado

Elementos principales de un cableado estructurado

El Cableado estructurado, es un sistema de cableado capaz de integrar tanto a los servicios de voz, datos y vídeo, como los sistemas de control y automatización de un edificio bajo una plataforma estandarizada y abierta. El cableado estructurado tiende a estandarizar los sistemas de transmisión de información al integrar diferentes medios para soportar toda clase de tráfico, controlar los procesos y sistemas de administración de un edificio.

Estándares EIA/TIA 568

El estándar EIA/TIA 568 (EIA: Asociación de Industrias electrónicas, TIA: Asociación de Industria de Telecomunicaciones), se desarrolló para la instalación de cableados estructurados en edificios comerciales. Su propósito es considerar ciertas normas de acuerdo al medio de transmisión para que el cableado pueda ser certificado. Los elementos del cableado que propone son:

1.- Par trenzado, cuatro pares, sin blindaje (UTP) de 100 ohmios, 22/24 AWG
2.- Par trenzado, dos pares, con blindaje (STP) de 150 ohmios, 22 AWG
3.- Fibra óptica, dos fibras, multimodo 62.5/125 mm

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5e similar al Commscope 55N4. El cable coaxial de 50 ohmios se acepta pero no se recomienda en instalaciones nuevas.

Métodos de transmisión

Existen dos métodos de transmisión en las redes: banda base y banda ancha.

El método de banda base define que solamente una señal digital puede viajar por el medio. Cada señal transmitida utiliza el ancho de banda total del medio.

Los cables coaxiales, la fibra óptica y el cable UTP para banda base son los más comunes para este tipo de transmisión.

El método de banda ancha permite que varias señales puedan viajar por el mismo medio, por ejemplo un cable coaxial de televisión por cable con un ancho de banda de 500 MHz puede llevar muchos canales de televisión, cada uno codificado a diferentes MHz de ancho de banda; la información se modula antes de transmitirla.

Los cables de fibra óptica y coaxial para banda ancha son los más comunes para este tipo de transmisión.

Cable Coaxial

El cable coaxial que se usa en redes de área local es del tipo banda base, su construcción es muy parecida al cable coaxial de banda ancha, pero las principales diferencias son: el diámetro del cable, su cubierta y la impedancia. Este tipo de cable está en desuso para Redes LAN.

Tipo de cable	RG-58 A/U, RG8 o RG11
Velocidad Máxima de transferencia	10 Mbps
Impedancia	50 Ω
Distancia máxima de segmento	185 – 500 m
Costo	Bajo
Inducción de ruido	Baja

Tabla 3-2 - Características del cable coaxial de banda base

Cable UTP

El cable de par trenzado (UTP) se utiliza para los sistemas telefónicos. Generalmente el cable UTP para redes de área local, está formado por cuatro pares cubiertos con forro de plástico, algunos cables tienen además un recubrimiento metálico que ayuda a incrementar la velocidad de transmisión de datos y protegerlo de ruido exterior (STP - Shielded Twisted Pair).

Existen dos tipos de cables: UTP y STP, en los cuales la diferencia principal es el recubrimiento que tienen para aislar el ruido, dependiendo de la categoría del cable se puede obtener altas velocidades.

Actualmente hay varias categorías de este tipo de cables, cada categoría define la velocidad de transmisión.

Actualmente las categorías son:

Categoría	Tipo	Ancho de banda	Longitud	Aplicaciones LAN	Comentarios
Cat 3	UTP	16 MHz	100m	10BaseT, 4 Mbps	Para cables telefónicos
Cat 4	UTP	20 MHz	100m	16 Mbps	Visto raramente
Cat 5	UTP	100 MHz	100m	100Base-Tx, ATM, CDDI	Comúnmente para LANs actuales
Cat 5e	UTP	100 MHz	100m	1000Base-T	Comúnmente para LANs actuales
Cat 6	UTP	250 MHz	100m	1000Base-T	Actualmente implementado en LANs
Cat 6 a	STP	550 MHz	100m	T10GBase-T	Actualmente implementado en LANs
Cat 7	STP	600 MHz	100m	10GBase-T	Emergente

Tabla 3-3 – Categorías Cable UTP

Fibra Óptica

Los cables de fibra óptica se usan para transmitir señales digitales de datos en forma de pulsos modulados de luz. La fibra se usa para transmisiones de banda base y banda ancha.

En una conexión con fibra óptica se ocupan dos fibras, una para transmisión y otra para recepción. La velocidad de transmisión va de 100Mbps hasta 10Gbps (Gigabits por segundos) dependiendo de las características tecnológicas de la fibra.

Existen dos tipos de fibra óptica: monomodo (single mode) y multimodo (multi mode). La fibra monomodo utiliza un rayo láser para alcanzar grandes distancias, la fibra multimodo usa un LED que emite múltiples rayos de luz, y esta fibra se ocupa para distancias mas cortas que van desde los 100m hasta 10km.

Estándares de cableado

Los estándares definen las características de los materiales que se utilizan en los cableados de redes de área local, como son:

- Tipo de cable
- Velocidad de transmisión
- Número de cables, su resistencia y la máxima distancia permitida
- Conectores

En general los sistemas de cableados se componen de cables de cobre y de fibra óptica, cajas de interconexión, adaptadores y equipos estándar para cableado en edificios, estipulados por la EIA/TIA 568.

Un sistema de cableado estructurado se refiere a la administración eficiente en su instalación y al estricto control de los puertos que serán utilizados en la puesta en marcha de un sistema de redes de voz y datos.

3.7. Tecnologías de Redes de Área Local

En la actualidad existen varias tecnologías de redes de área local, como Ethernet, Token Ring, FDDI, ATM. Estas tecnologías tienen métodos de acceso diferentes y por lo tanto operan de manera diferente.

La operación de estas tecnologías están reguladas por diversos organismos internacionales como la ISO, IEEE, etcétera, debido a que son desarrollos tecnológicos de diversas compañías.

3.7.1. Ethernet

La tecnología Ethernet es la más usada actualmente, la primera implementación data del año de 1970, por Robert Metcalfe y David Boggs de la compañía Xerox, conectaron 100 computadoras en una rea de 100km, y su velocidad de transmisión fue de 2.94 Mbps.

Se utiliza en topologías de bus y estrella, normalmente se usa en banda base y el método de acceso a la red es CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Su función es escuchar el medio para asegurase que nadie este transmitiendo en ese momento. Si nadie lo está haciendo, comienza la transmisión; si el medio está ocupado, espera un tiempo aleatorio y vuelve a intentar. Si dos dispositivos transmiten al mismo tiempo, ocurre una colisión; los dispositivos retransmiten la información cuando ocurre una colisión, pero antes de hacerlo esperan un tiempo aleatorio.

En la tecnología Ethernet existen varios sub-estándares de la IEEE 802.3 relacionados con los medios de transmisión y su velocidad, los más comunes son los siguientes:

10Base5: Significa que puede transmitir a 10 Mbps, en una sola banda y con una distancia máxima de 500mts, usa cable coaxial grueso, los dispositivos conectados debe tener por lo menos 2.5mts de separación.

10Base2: Significa que puede transmitir a 10 Mbps, en una sola banda y con una distancia máxima de 185mts, usa cable coaxial delgado, el máximo número de nodos en red es de 30 por segmento.

10BaseT: Significa que puede transmitir a 10 Mbps, en una sola banda y con una distancia máxima de 100mts del concentrador al dispositivo de red, usa cable tipo UTP o STP.

10BaseFL: Significa que puede transmitir a 10 Mbps, en una sola banda y con una distancia de hasta 2km, generalmente se usa como backbone y usa fibra óptica multimodo como medio de transmisión.

100Base-TX: Significa que puede transmitir a 100 Mbps, en una sola banda y con una distancia máxima de 100mts del concentrador al dispositivo de red, usa cable tipo UTP o STP categoría 5 en adelante.

100Base-FX: Significa que puede transmitir a 100 Mbps, en una sola banda y con una distancia de hasta 2km, generalmente se usa como Backbone y usa fibra óptica multimodo como medio de transmisión.

1000Base-T: Significa que puede transmitir a 1000 Mbps, en una sola banda y con una distancia máxima de 100mts del concentrador al dispositivo de red, usa cable tipo UTP o STP categoría 5e en adelante.

1000Base-X: Significa que puede transmitir a 1000 Mbps, en una sola banda y con una distancia de 10 a 20km con fibra mono-modo, con fibra multimodo de 220 hasta 600 mts, generalmente se usa como backbone.

3.7.2. Token Ring

Es una arquitectura de red desarrollada por IBM en los años 70's. IBM coloco en el mercado las redes Token Ring que fueron competidores numero uno de las redes Ethernet. Las redes Token Ring son probabilísticas y su método de acceso es Token Passing, y está diseñado para operar con redes con topología en anillo.

Estas redes están en desuso debido a la popularidad y a las ventajas que presenta la tecnología Ethernet.

3.7.3. FDDI

El estándar FDDI (Fiber Distributed Data Interface) opera a una velocidad de 100Mbps usando cable de fibra óptica. FDDI usa conexiones full-duplex, punto a punto de fibra óptica, en sus inicios el uso de esta tecnología solamente se empleaba backbones de edificios o campus (columna vertebral) que demandaban mayores anchos de banda y grandes distancias.

Las redes FDDI se componen de un doble anillo, el cual ayuda a tener redundancia en caso de que se presenten fallas en la red.

3.7.4. ATM

ATM (Asynchronous Transfer Mode) es un acrónimo en la nomenclatura de redes. Las redes ATM son consideradas redes de tercera generación. La primera referencia de ATM tiene lugar en los años 60 cuando un norteamericano de origen oriental de los laboratorios Bell describió y patento un modo de transferencia no síncrono. Sin embargo ATM no se hizo popular hasta 1988 cuando el CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) decidió que sería la tecnología de conmutación de las futuras redes ISDN en banda ancha.

El despliegue de la tecnología ATM no fue el esperado por sus promotores. Las velocidades de 622 Mbps han sido superadas. ATM no es la opción para redes actuales y futuras.

3.8. Protocolos de Comunicaciones

Para las redes de computadoras, un protocolo es el conjunto de normas que permiten que dos o más computadoras puedan comunicarse.

3.8.1. TCP/IP

Es uno de los protocolos más antiguos en los estándares de redes interconectadas. TCP/IP se desarrollo por la Agencia de Proyectos de Investigación Avanzada de la Defensa de Estados Unidos de America (DARPA: Defense´s Advanced Research Project Agency).

Es un protocolo flexible y permite la transmisión con control de errores entre diferentes sistemas. Como es un protocolo de transferencia de información, puede enviar grandes cantidades de información a través de redes no confiables, garantizando que va a ser recibida sin errores al destino final.

Las redes TCP/IP permiten que la información pueda enviarse de un sistema a otro, aunque sean de diferentes fabricantes; por ejemplo una PC con sistema operativo Windows XP puede comunicarse con una computadora con sistema operativo Linux, siempre y cuando ambas utilicen el protocolo de comunicaciones TCP/IP.

3.8.2. NetBEUI

Proviene de una extensión de la interfaz de usuario NetBIOS y fue introducido por IBM en 1985 como un protocolo pequeño, rápido y eficiente. NetBEUI fue optimizado para usarlo en redes con 20 a 200 computadoras conectadas que formarían grupos de trabajo. Las ventajas de este protocolo son: rápido en segmentos pequeños y usan muy poca memoria; las desventajas son: no es enrutable y su rendimiento es muy pobre en redes WAN.

Con la aparición de NetBIOS sobre TCP/IP ha causado que NetBEUI actualmente ya no sea tan popular.

3.8.3. IPX/SPX

Es el protocolo de comunicaciones de la redes tipo NetWare, de la compañía Novell. Es un protocolo propietario y solamente se usa en redes NetWare. El uso de este protocolo a disminuido desde que Internet hizo popular el protocolo TCP/IP.

Ahora es posible utilizar productos de Novell sin IPX, debido a que algunas versiones de sus productos soportan ambos protocolos IPX y TCP/IP.

3.9. Equipos de comunicaciones

Son los diferentes componentes que interconectan las redes de área local para poder administrarlas, expandirlas, combinar diferentes tecnologías, etcétera, estos se conocen como equipos de comunicaciones.

Los más usuales se encuentran los concentradores, módems, repetidores, puentes (bridges), enrutadores y las tarjetas de red.

3.9.1. Concentradores

Los concentradores son dispositivos con tecnología de conmutación de paquetes (Paquet Switching), pueden interconectar un gran volumen de computadoras. Son equipos muy usados en compañías que requieren muchos nodos de red, la mayoría de los concentradores ofrecen herramientas de administración y monitoreo, para diagnosticar loas condiciones de la red.

3.9.2. Repetidores

Son equipos diseñados para amplificar la señal que se recibe, su principal problema es que también amplifican el ruido, por lo que se debe tener cuidado al instalar uno de ellos. Únicamente funciona con redes idénticas.

3.9.3. Puentes

Son dispositivos de hardware con software integrado, y son necesarios para unir dos o más tipos de redes. Pueden interconectar redes diferentes debido a que usan software para conectarlos. Los puentes transparentes examinan las direcciones físicas de destino y deciden si los paquetes son transmitidos al otro lado de la red, sin que el usuario tenga que programar los equipos.

3.9.4. Enrutadores

Estos equipos trabajan el nivel 3 del modelo OSI (nivel de red: Network Layer). Trabajan con protocolos superiores como TCP/IP, XNS, NetBIOS, etcétera.

Algunos enrutadores sofisticados son capaces de administrar el enrutamiento de paquetes de una red a otra, independientemente del tipo de redes que se están usando y usan software mas sofisticado.

3.9.5. Switches

Es un dispositivo de interconexión de redes de computadoras, opera en la capa 2 del modelo OSI (Data Link Layer). Funciona de manera similar a los puentes y puede interconectar dos o más segmentos de red.

Los switches a diferencia de los concentradores, mejoran el rendimiento y la seguridad de las redes de área local.

4

Redes de Área Local Inalámbrica (WLAN).

En el capitulo anterior revisamos información sobre los temas básicos de redes en general, en el presente capitulo revisaremos, ya más específicamente datos respectivos a redes inalámbricas, Abarcaremos tanto definiciones de fenómenos físicos que son importantes considerar para una red inalámbrica, como conceptos básicos de equipos configuraciones y estándares.

4.1. Conceptos Básicos de las Redes Inalámbricas

Redes inalámbricas

Las redes inalámbricas son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Tienen ventajas como la rápida instalación de la red sin la necesidad de usar cableado, permiten la movilidad y tienen menos costos de mantenimiento que una red convencional.

Radiofrecuencia

Las conexiones inalámbricas Wi-Fi (Wireless Fidelity) realizan la comunicación a través de la radiofrecuencia, estas son ondas electromagnéticas que viajan de un lugar a otro a través de un medio como el aire, e incluso el vacio pero sin depender de él.

Para explicar el comportamiento de las ondas de radio, es necesario conocer primero qué son las ondas.

Las ondas de radio, son ondas electromagnéticas que se propagan sin necesidad de un medio físico que las soporte. Para entender el concepto de onda, imaginemos una piedra tirada en el agua: desde el lugar donde cayó, empiezan a surgir ciertas “deformaciones”, que se conocen como ondas; en este caso en particular, son ondas mecánicas, por que se generan debido al movimiento de algún objeto o de su medio de propagación (el agua).

Las ondas electromagnéticas, en particular, se generan y propagan mediante la oscilación de campos eléctricos y magnéticos. No olvidemos que las cargas eléctricas (electrones) en movimiento producen un campo magnético.

Si inyectamos una cantidad suficiente de electrones en forma periódica en un alambre, en cierto momento tendremos, en un extremo del alambre, la mayoría de las cargas negativas, y los electrones tenderán a ir hacia ese lado. Si esto sucede de manera periódica, los vectores del campo eléctrico abandonarán el alambre hacia el espacio que lo rodea, y entonces generará una onda electromagnética.

Propiedades de las ondas electromagnéticas

Las ondas electromagnéticas poseen ciertas propiedades que las definen:

Frecuencia: Es la cantidad de ondas completas que pasan por un punto fijo en un segundo. La medida que se utiliza para referenciarla es el Hertz (Hz).

Longitud de onda: Es la distancia desde un punto de la onda hasta el punto siguiente equivalente (por ejemplo, de pico a pico) y su unidad de medida es el metro (m).

Velocidad: En las ondas electromagnéticas, se refiere a la velocidad de propagación de la luz, 300,000 km/s aproximadamente.

Amplitud de la onda: Es su altura desde su punto medio hasta uno de sus picos. Debemos tener en cuenta que, a mayor frecuencia e igual potencia y ganancia, la distancia que cubre la onda disminuye.

La forma en que se interrelacionan se puede determinar mediante la ecuación:

$$V=F*\lambda$$

Fenómenos físicos que afectan las ondas electromagnéticas

Existen fenómenos que pueden afectar a una señal de radiofrecuencia y pueden causarnos varios problemas. Existen tres fenómenos que modifican las ondas de radiofrecuencia: absorción, reflexión e interferencia.

Absorción

Si en su camino una onda debe atravesar un objeto, irremediablemente se verá afectado por el fenómeno de absorción, que hará que parte de la potencia se pierda en el objeto y, por tanto, la potencia total de la señal disminuya. La cantidad de potencia perdida estará dada por el coeficiente de absorción del objeto. A mayor coeficiente de absorción, mayor será la pérdida de potencia.

En este caso, al hacer uso de las microondas en la frecuencia de los 2.4 GHz, los objetos que mayor coeficiente de absorción poseen son el metal y el agua (en cualquiera de sus estados). Por lo tanto es común que la calidad del enlace disminuya y, entonces, tengamos menor velocidad de conexión en los días de lluvia o con un índice de humedad muy alto.

Es importante notar que, dada la gran cantidad de agua que poseen los seres vivos en su composición, incluyendo los árboles, hay que tratar de evitar lo más posible que la señal deba atravesarlo, lo cual, en algunos casos, será imposible.(Véase Figura 4-1)

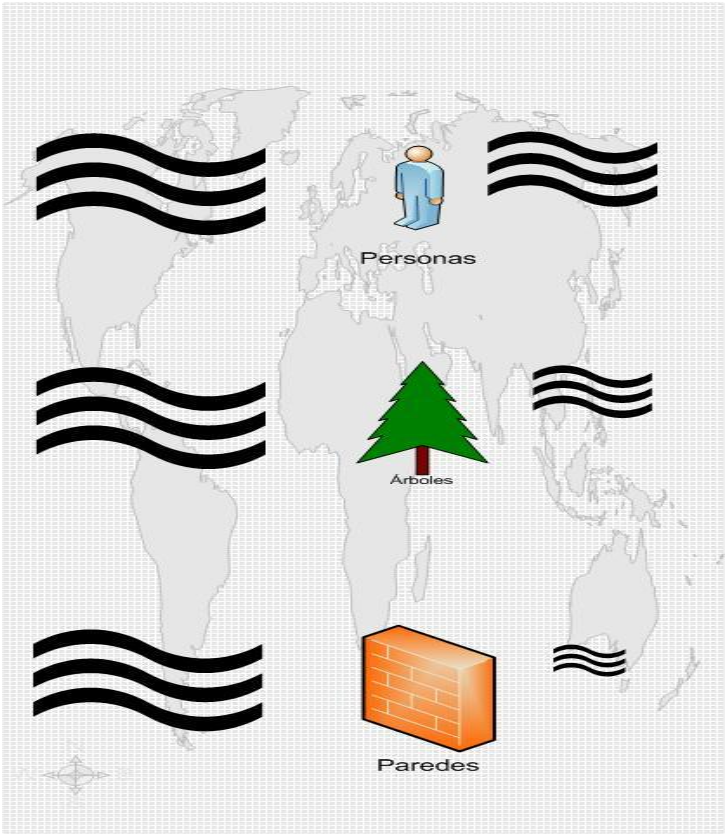


Figura 4-1

Fenómeno de Absorción de una onda al incidir sobre diferentes objetos.

Reflexión

Otro fenómeno que podemos observar es el de la reflexión. Cuando una onda incide sobre una superficie que tiene un alto índice de reflexión (como el metal y el agua), la señal reflejada tendrá el mismo ángulo de salida que el de entrada con respecto al objeto reflector. Para comprenderlo mejor, podemos decir que si una onda incide en un objeto reflector con un ángulo de 45°, la onda reflejada también tendrá 45°. Este fenómeno se utiliza en las antenas parabólicas para orientar la señal en una dirección concreta.

Interferencia

Esta genera una distorsión de la señal que puede llegar a comprometer seriamente el enlace. También puede suceder que la interferencia mejore la señal. Para comprender esto, debemos saber que existen dos clases de interferencia: una constructiva y una destructiva.

Una interferencia constructiva se da cuando los picos de onda de diferentes señales coinciden. Esa coincidencia dará como resultado una onda con el doble de amplitud. Para que esto suceda, las longitudes de onda de las dos señales deben ser iguales, así como también deben tener una relación de fase fija.

Al contrario, en una interferencia destructiva, si el pico de una onda coincidió con el valle de otra, se produce una "aniquilación" total de la señal.

4.2. Clasificación de la Redes inalámbricas

Los tipos de redes inalámbricas dependen de su alcance y del tipo de onda electromagnética utilizada. Según su tamaño encontramos las siguientes redes, de menor a mayor alcance.

WPAN

(Wireless Personal Area Network):

Este tipo de red se utiliza con tecnologías como HomeRF, Bluetooth, IrDa, ZigBee y RFID. Es una red personal de poco alcance, las tecnologías que la utilizan pueden conectar los teléfonos móviles de la casa y las computadoras personales mediante un aparato central.

WLAN

(Wireless Local Area Network):

En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HiperLAN (High Performance Radio LAN), o tecnologías basadas en Wi-Fi (Wireless-Fidelity).

WMAN

(Wireless Metropolitan Area Network, Wireless MAN):

La tecnología más popular que utiliza esta red es WiMax (Worldwide Interoperability for Microwave Access), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. Es muy parecido a Wi-Fi, pero tiene más cobertura y ancho de banda. Otro ejemplo es LMDS (Local Multipoint Distribution Service).

WWAN

(Wireless Wide Area Network, Wireless WAN):

Es la red que se utiliza para los teléfonos móviles de segunda y tercera generación (UMTS) y para los móviles GPRS (tecnología digital)

4.3. Topologías de la Redes Inalámbricas

Las redes inalámbricas, al igual que las cableadas, sirven para interconectar no solo computadoras, sino también cualquier otro tipo de equipo informático que se le pueda instalar un dispositivo inalámbrico. Este es el caso de las agendas electrónicas PDA, las impresoras o las cámaras digitales. A pesar de ello, no cabe duda de que el uso fundamental que se le da a una red inalámbrica es la interconexión de computadoras y el acceso a internet.

Topología en modo Ad HOC

IBSS (Independent Basic Service Set):

Es una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos Wi–Fi en cada computadora, las cuales se comunican unas con otras directamente, sin necesidad de que existan puntos de acceso intermedios. (Véase Figura 4-2)

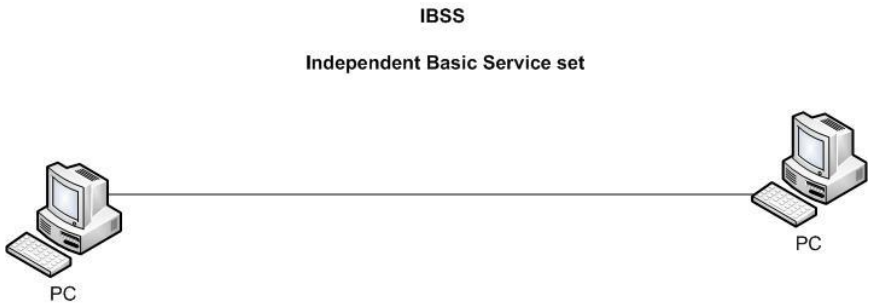


Figura 4-2 Topología Ad Hoc

Topología en modo Infraestructura

BSS. En esta configuración, además de las tarjetas Wi -Fi en las computadoras, se necesita disponer de un equipo conocido como punto de acceso, el cual lleva a cabo una coordinación centralizada de la comunicación entre las distintas terminales de red. (Véase Figura 4-3)

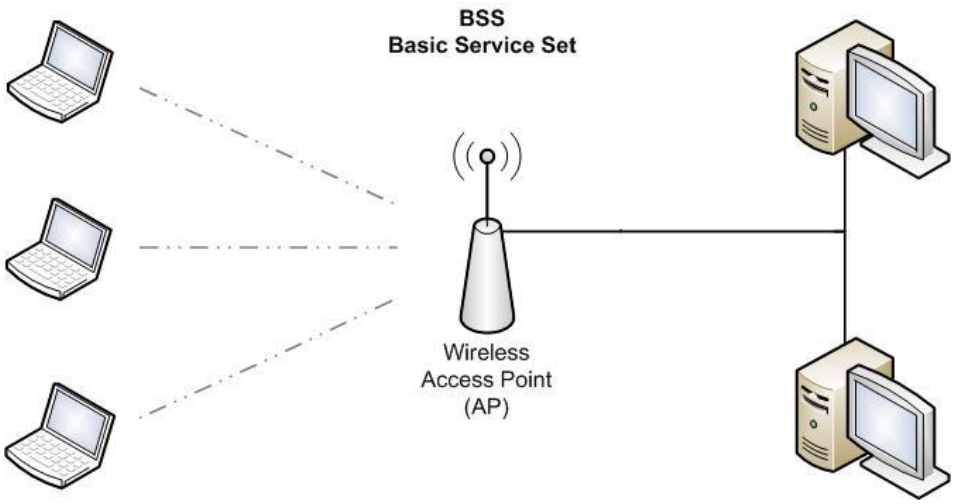


Figura 4-3 Topología en modo infraestructura.

Topología en modo ESS

Esta configuración permite unir distintos puntos de acceso para crear una red inalámbrica con una amplia cobertura. Una red ESS está formada por múltiples redes BSS. Las distintas redes BSS se pueden poner pegadas unas a otras para conseguir tener una comunidad de servicio en toda la red ESS. (Véase Figura 4-4)

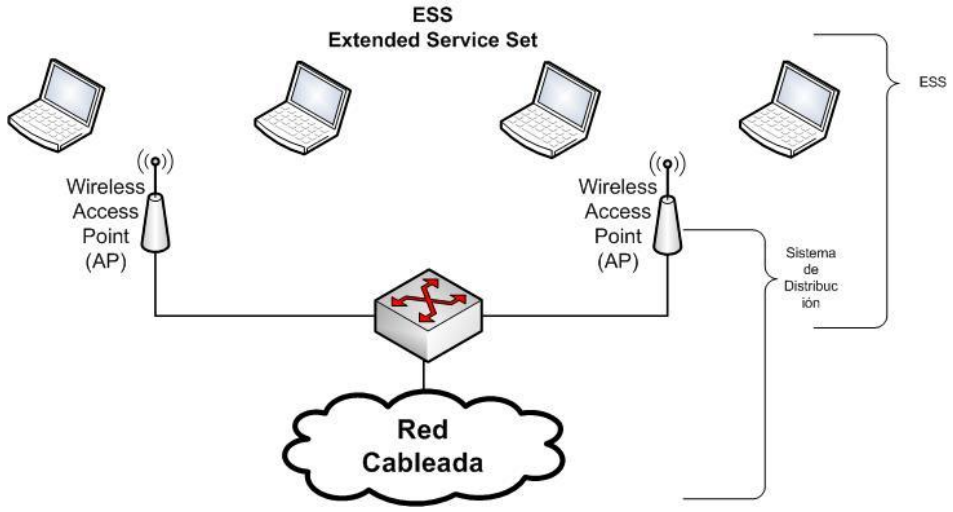


Figura 4-4. Topología ESS

Desde el punto de vista de las terminales, las configuraciones BSS y ESS son la misma. Por otro lado, una terminal no puede estar configurada en modo ad hoc e infraestructura a la vez; lo que si se puede es configurar la terminal de distinta forma dependiendo de las necesidades de la red.

4.4. Tecnologías y estándares de las Redes Inalámbricas

Existen varias tecnologías competidoras WLAN, y se ha creado un poco de confusión e información inexacta en el mercado en cuanto a los aspectos relacionados con un “estándar” WLAN. Vale la pena notar que hay una diferencia considerable en el grado hasta el cual cada uno de estos estándares ha sido adoptado no sólo por los desarrolladores de tecnología, sino por el mercado mismo.

IrDA

(Infrared Data Association)

En la actualidad ya no se le considera competencia a este estándar ya que las características con las que cuenta son inferiores a las que ofrecen los otros tres estándares, como la imposibilidad de transmitir voz, corto alcance y limitada transferencia de datos

IrDA . Actualmente tiene creados dos estándares:

IrDA-Control que es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos.

IrDA-Data que está orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de un metro y a velocidades que van desde los 9.6 Kbps hasta los 16 Mbps.

Home RF

(Home Radio Frequency)

Compaq, HP, IBM, Intel, Microsoft y Promix entre otros, establecieron un grupo de trabajo para desarrollar y promover la tecnología HomeRF y seleccionó al mercado residencial como su objetivo principal.

HomeRF saco su versión 2.0 de su protocolo SWAP (Shared Wireless Access Protocol-Protocolo de Acceso Compartido Inalámbrico). SWAP trabaja en la banda de frecuencia de 2.4 GHz con FHSS (Frequency Hopping Spread Spectrum, “Espectro Expandido por Salto de Frecuencia”), y permite configuraciones de comunicaciones punto a punto y comunicaciones con punto de comunicación central. SWAP 2.0 permite transmitir datos hasta 10 Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene alcance de 50 metros y una potencia de 100 mW.

Bluetooth

Bluetooth utiliza la técnica **FHSS** en la banda de frecuencia de 2.4 GHz. Por otro lado, puede transmitir tanto voz como datos.

IBM, mediante el mercado BlueTooth, ha perseguido esencialmente el mercado comercial/ventas. HomeRF ha ofrecido productos en el mercado con precios muy bajos, mientras que los equipos 802.11 son un tanto más costosos.

Esta diferencia enorme en los precios, generalmente refleja la orientación de los mercados; en otras palabras, el equipo de costo muy bajo, por lo común incluye características de seguridad mínimas, desempeño bajo y niveles muy inferiores de interoperabilidad y se usan en ambientes donde no se requiere que el radio opere como un elemento de red sofisticada, como es el caso de las empresas comerciales, mercados financieros y otros negocios.

Es posible que el BlueTooth haya tenido la cobertura más grande por parte de la prensa, pero es por mucho el que menor número de dispositivos tiene en el mercado y casi siempre está integrado dentro de otro dispositivo como un PDA o un teléfono celular.

	HomeRF	BlueTooth	802.11
Capa Física	FHSS	FHSS	FHSS,DSSS,IR
Saltos de Frecuencia	50 saltos por segundo	1,600 saltos por segundo	2.5saltos por segundo
Potencia de transmisión máxima	100mW	100mW	800mW
Velocidades de datos	10 Mbps	1 Mbps	11 Mbps
Número máximo de dispositivos	Hasta 127	Hasta 26	Hasta 256
Seguridad	Formato Blowfish	0, 40 y 64 bits	40 y 28 bits RCS TKIP MIC, SSN
Rango	150 pies	30 pies	400 pies en exteriores, 1000 pies
Versión actual	V2.0	V1.0	V1.0
Costo	Ni más ni menos costoso	Menos costoso	Más Costoso
Tamaño físico	Ni mayor ni menor	El más pequeño	El más grande
Alcance exterior al Hogar	No	No	Si

Tabla 4-1 - Comparativa de Tecnologías Inalámbricas

El estándar 802.11

Una de las razones importantes para obtener un estándar es que el equipo que proporcione un proveedor A funcione con el equipo del proveedor B. La compañía que apoya el estándar con frecuencia toma en cuenta una ganancia financiera considerable, debido a que por lo general ofrece un elemento o característica importante que se requiere como parte del estándar.

Las compañías grandes prefieren los productos basados en estándares debido a que normalmente pueden vender más productos a un solo cliente, en especial cuando el cliente es grande. Los clientes grandes optan por los estándares debido a que proporcionan estabilidad a los diseños de productos básicos y aseguran la interoperabilidad a medida que sus redes crecen y migran.

Es importante que solo uno de los competidores pueda soportar lo que en realidad se puede llamar banda ancha, y ése es el IEEE 802.11.

4.5. Protocolos o Estándares de las Redes inalámbricas IEEE 802.11

IEEE 802.11, o simplemente Wi-Fi, es un protocolo de comunicaciones IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y enlace de datos), especificando como debe de funcionar en una WLAN.

Su aparición se remonta a 1997, cuando ofrecía velocidades de hasta 2 Mbps sobre la frecuencia ISM de 2,4 GHz. Las bandas ISM (Industrial Scientific and Medical) son espectros de radiofrecuencia que están libres de licencias y pueden ser usados por cualquiera sin pedir autorización.

Existen diferentes implementaciones del protocolo 802.11 que fueron surgiendo con el correr de los años, que tienen características específicas, y en algunos casos, no son compatibles con las demás.

4.5.1. La Capa de Control de Acceso al Medio

La capa MAC es un subconjunto de enlace, que a su vez es adyacente a la capa física en una red basada en IP. La Capa 1 en una red 802.11 realiza por lo menos tres funciones esenciales:

1. Como la interfaz entre la capa MAC en dos o más ubicaciones geográficas. Estas ubicaciones normalmente sólo están a pocos cientos de pies o menos distancia.
2. Realizan la detección real de sucesos CSMA/CD, mismos que ocurren dentro de la capa MAC.
3. Efectúan la modulación y demodulación de la señal entre dos puntos geográficos en los que residen equipos 802.11. Este esquema de modulación puede ser DSSS (Direct Sequence Spread Spectrum, "Espectro Ensanchado por Secuencia Directa"), o FHSS.

El estándar 802.11 define una técnica de cambio de velocidad que permite a las redes reducir las velocidades de datos a medida que ocurren cambios en la distancia, calidad y fuerza de la señal. Las velocidades de datos de 802.11b IEEE pueden ser tan altas como 11 Mbps o tan bajas como 1 Mbps con modulación DSSS, en tanto que las velocidades de datos moduladas con FHSS pueden ser de 1 ó 2 Mbps. El estándar también permite la compatibilidad entre los radios 802.11a y 802.11b.

La capa MAC es una subcapa de la Capa 2 del modelo OSI y controla la conectividad de dos o más puntos a través de un esquema de direcciones. Cada computadora portátil o punto de acceso tiene una dirección MAC (Media Access Control address o dirección de control de acceso al medio). El estándar 802.11 IEEE define la forma en que funciona esta asignación de direcciones además de la manera en que operan algunos aspectos de la Capa 1.

De hecho define lo siguiente:

- Las funciones que se requieren en un dispositivo compatible con 802.11 para operar en una red de igual a igual o integrado en una WLAN existente.
- La operación del dispositivo 802.11 dentro del rango de otros dispositivos 802.11 y la forma en que la tarjeta cliente migraría físicamente de un punto de acceso a otro (roaming).
- Servicios de control de acceso y entrega de datos al Nivel MAC para las capas superiores de la pila de protocolos de red.
- Varias técnicas de interfaz de señalamiento en la capa física.
- Privacidad y seguridad en los datos del usuario que se transfieren a través del medio inalámbrico.

Lo que hace que una WLAN sea diferente de una LAN Ethernet es, obviamente, la capacidad de los usuarios de trasladarse de un punto de la red a otro y seguir conectados. Ésta es la característica más importante de una WLAN y es la que representa la mayor diferencia con una LAN Ethernet.

La forma en la que opera MAC en el estándar 802.11 es lo que permite que los niveles más altos del modelo OSI funcionen adecuadamente. En otras palabras, la capa MAC es la que controla los aspectos de movilidad en una red 802.11.

Es por esta razón que una capa MAC 802.11 está obligada a hacerse cargo de ciertas funcionalidades que normalmente son responsabilidad de capas más altas del modelo OSI, por ejemplo, la capa de sesión (Capa 5), que controla el inicio y la terminación de sesiones. En el estándar MAC 802.11, el flujo de información se realiza mediante un método del mejor esfuerzo, que también se conoce como "sin conexión". Los enlaces sin conexión son en los que el extremo receptor del enlace no verifica la recepción de los datos con el enlace transmisor. La técnica que usa la capa MAC se conoce como Accesos Múltiples de Sensor de Portadora con Detección de Colisiones (CSMA/CD: Carrier Sense Multiple Access with Collision Detection) que es una técnica que requiere que el transmisor "escuche" lo que ocurre en el entorno local, para asegurarse de que no existen otras transmisiones en la frecuencia asignada. La detección real se efectúa en la CAPA 1, pero el control del tiempo para las transmisiones se controla en la CAPA MAC.

Otra Función que proporciona la capa MAC 802.11 es la de seguridad, la que normalmente se controla en la capa de presentación (Capa 6).

4.5.2. Estándar 802.11a

Trabaja sobre la banda ISM de 5 GHz (de 5150 a 5850 MHz), y puede transmitir hasta 54 Mbps en canales separados de 10 MHz; su longitud de onda es del orden de 5 a 6 cm. Las ventajas más importantes que tiene la norma "a" sobre las diferentes implementaciones de 802.11, son su capacidad para 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto, y su inmunidad a la interferencia radial causada por los teléfonos, los productos que emplean Bluetooth y otros dispositivos inalámbricos que comparten la banda de 2,4GHz.

Su uso no está muy extendido, ya que no es compatible con las otras normas. Si bien existen equipos multinorma, pero suelen ser muy costosos.

4.5.3. Estándar 802.11b

Esta norma fue la que inicio el "boom" de las comunicaciones inalámbricas. Trabaja con una frecuencia que va de 2400 MHz a 2484 MHz. Tiene una velocidad de 11Mbps y una longitud de onda de aproximadamente 12.5 cm. La particularidad que tiene la distribución de los canales en esta norma es que cada uno de ellos tiene un ancho de 22MHz, pero la separación entre canales es de solo 5MHz, de modo que los canales quedan solapados.

Podemos ver la imagen de distribución de canales (FIG 2-11) para hacernos una idea de cómo funciona. Como pueden apreciar, por ejemplo, los canales 1, 6 y 11 no se superponen. Debido a esto si hay más de una red cerca, hay que tratar de de elegir canales que no se repitan, para evitar interferencias. (Véase Figura 4-5)

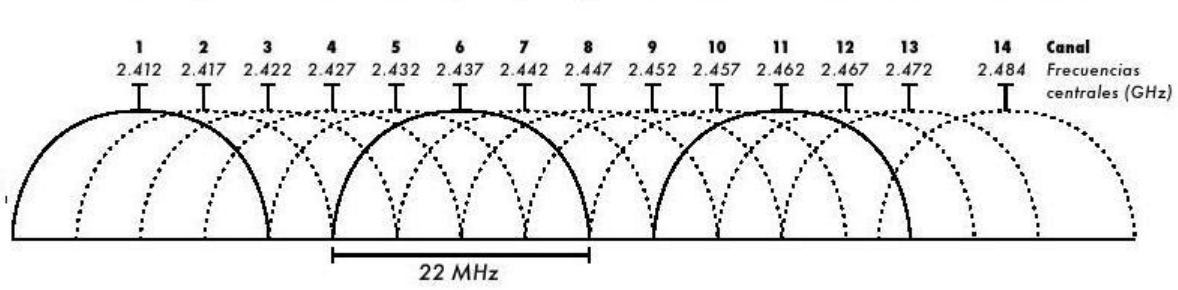


Figura 4-5 Solapamiento de canales

4.5.4. Estándar 802.11g

Al igual que el estándar "b", la norma "g" utiliza la frecuencia de 2.4 GHz, pero en una velocidad de 54Mbps, lo cual la coloca a la altura de la norma "a", pero teniendo compatibilidad con la "b". Esto aseguro su rápida aceptación.

4.5.5. Estándar 802.11e

Esta norma introduce calidad de servicio (QoS – Quality Of Service – "Calidad de Servicio") en los enlaces para mejorar las respuestas en entornos que trabajan en tiempo real.

4.5.6. Estándar 802.11 i

Es un estándar de seguridad para WLAN. Combina el uso de 802.11 y protocolos de cifrado TKIP/CCMP, que ofrece autentificación de usuario (no de dispositivo), confiabilidad e integridad de los datos.

4.5.7. Estándar 802.11 n

Es un relativamente nuevo estándar de las redes inalámbricas, y el MIMO (Multiple Input – Multiple Output) solo es una de las características del mismo. Suministra velocidades superiores a 100 Mbps lo cual duplica la velocidad de 802.11g y 802.11a, que es de 54 Mbps.

Las ondas de Radio Frecuencia son "Multi-Señal" y siempre existe una onda primaria y varias secundarias. Hasta ahora, sólo se aprovechaba la onda primaria y las otras eran vistas como "interferencias" o "ruidos". El algoritmo MIMO, envía señal a dos o más antenas y luego las recoge y re-convierte en una. El estándar Wi-fi 802.11n funcionará en las bandas de 10, 20, o 40 MHz y se alcanzarán velocidades superiores a 100 Mbps. Estas podrían superar también los 300 Mbps.

Estándar	Frecuencia Portadora	Velocidad de datos	Resumen
802.11 a	5.1 - 5.2 GHz 5.2 - 5.3 GHz 5.7 – 5.8 GHz	54 Mbps	La potencia máxima es de 40 mW en la banda 5.1, 250 mW en la banda 5.2 y 800 mW en la banda 5.7 (En E.U.)
802.11 b	2.4 – 2.485 GHz	11Mbps	Es el estándar más conocido
802.11 d	N/D		Múltiples dominios reguladores
802.11 e	N/D	N/D	Calidad de servicio
802.11 f	N/D	N/D	Protocolo de conexión entre puntos de acceso IAPP.
802.11 g	2.4 – 2.485 GHz	54 Mbps	
802.11 h	N/D	N/D	Selección dinámica de frecuencia DFS
802.11 i	N/D	N/D	Seguridad.
802.11 n	2.4 y 5 GHz simultáneamente	300 Mbps	MIMO (Multi-In, Multi-Out) generando canales de tráfico simultáneos entre las diferentes antenas de los productos 802.11n Canales de 10, 20 y 40 MHz (Lo que permite incrementar enormemente la velocidad)

Tabla 4-2 – Estándares IEEE 802.11

4.6. Uso eficiente del rango y cobertura de la señal

Los estándares 802.11a, 802.11b y 802.11g, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Estándar	Frecuencia	Velocidad	Rango
WiFi a (802.11a)	5 GHz	54 Mbps	100 m
WiFi b (802.11b)	2,4 GHz	11 Mbps	100 m
WiFi g (802.11g)	2,4 GHz	54 Mbps	100 m

Tabla 4-3 Cobertura de los estándares

4.6.1. Estándar 802.11a

El estándar 802.11 tiene en teoría un flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo a un rango de treinta metros aproximadamente. El estándar 802.11a se basa en la tecnología llamada OFDM (multiplexación por división de frecuencias ortogonales). Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no solapados.

Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "banda dual".

Velocidad hipotética (en ambientes cerrados)	Rango
54 Mbps	10 m
48 Mbps	17 m
36 Mbps	25 m
24 Mbps	30 m
12 Mbps	50 m
6 Mbps	70 m

Tabla 4-4 Rangos de velocidades 802.11a

4.6.2. Estándar 802.11b

El estándar 802.11b permite un máximo de transferencia de datos de 11 Mbps en un rango de 100 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales).

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbps	50 m	200 m
5,5 Mbps	75 m	300 m
2 Mbps	100 m	400 m
1 Mbps	150 m	500 m

Tabla 4-5 Rangos de velocidades 802.11b

4.6.3. Estándar 802.11g

El estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM, es compatible con los dispositivos 802.11b con excepción de algunos dispositivos más antiguos.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbps	27 m	75 m
48 Mbps	29 m	100 m
36 Mbps	30 m	120 m
24 Mbps	42 m	140 m
18 Mbps	55 m	180 m
12 Mbps	64 m	250 m
9 Mbps	75 m	350 m
6 Mbps	90 m	400 m

Tabla 4-6 Rangos de velocidades 802.11g

4.7. Dispositivos de una Red Inalámbrica

Hay cuatro tipos genéricos de dispositivos de redes inalámbricas que pueden ser usados para los diferentes tipos de infraestructura de red inalámbrica, estos dispositivos son las tarjetas de red inalámbricas (PCMCIA, Mini-PCI, PCI), punto de acceso inalámbrico, puente inalámbrico y enrutador inalámbrico.

Tarjetas de Red inalámbrica

Se usan para conectar una computadora de escritorio o laptop a la red inalámbrica, debemos tomar en consideración el tipo de interfaz a donde vamos a instalar la tarjeta, esta puede ser: PCI, USB y PCMCIA.

Puntos de Acceso Inalámbrico

Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Se usan como un puente de capa 2 entre la red cableada y la red inalámbrica, y puede transmitir datos entre equipos conectados a la red de cable y los dispositivos inalámbricos. Los puntos de acceso inalámbricos se les asignan una dirección IP para que puedan ser configurados.

Puente Inalámbrico

Es un componente de hardware usado para conectar dos o más segmentos de red (redes o partes de una red), los cuales están físicamente y lógicamente (por protocolo) separados. Muchos enrutadores inalámbricos y puntos de acceso inalámbricos ofrecen un modo de puente o repetidor, ambos modos realizan una función común. La diferencia en modo de puente es que conecta diferentes tipos de protocolo y en modo de repetidor transmite el mismo tipo de protocolo.

Enrutador inalámbrico

Es un dispositivo construido con las mismas funcionalidades de un punto de acceso inalámbrico. Varios fabricantes introdujeron los enrutadores inalámbricos para agregar capacidades de ruteo en los puntos de acceso inalámbrico. Además de que proveen ruteo básico, comúnmente los enrutadores inalámbricos incluyen soporte para el protocolo de autoconfiguración dinámica de host (DHCP) y de traducción de direcciones de red (NAT).

Antenas

Una antena es un dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa. La antena de un equipo emisor radia ondas radioeléctricas, mientras que la antena de un equipo receptor las capta.

Una comunicación en la que la información fluye en ambas direcciones recibe el nombre de bidireccional. No obstante, cuando la transmisión y recepción no se efectúa simultáneamente, sino alternativamente, se obtiene lo que se conoce como comunicación SEMIDÚPLEX (half-duplex). Las comunicaciones Wi-Fi son bidireccionales semidúplex.

La teoría dice que una antena se instala para mejorar la señal que emitimos o recibimos. El mayor problema es la distancia de cable que une nuestra antena con nuestros puntos de acceso. El grave problema viene cuando comprobamos que una antena con un cable de, 2 metros conectada a nuestro punto de acceso no amplifica casi nada. Lo que ganamos con la antena, lo perdemos con el cable. De ese modo usaremos cables lo más cortos posible, de unos 30cm.

Tipos de Antenas.

Existen dos tipos genéricos de antenas: Omnidireccionales y direccionales.

Antenas Omnidireccionales:

Emiten señales en todas direcciones, además lo hacen de una forma muy homogénea, es decir, con prácticamente la misma potencia hacia todos lados. De este tipo son, por ejemplo, las antenas que vienen de fábrica en los puntos de acceso. Si pudiésemos ver la señal que generan estas antenas veríamos algo parecido a una Dona sobre el eje de la antena. (Véase Figura 5-6)

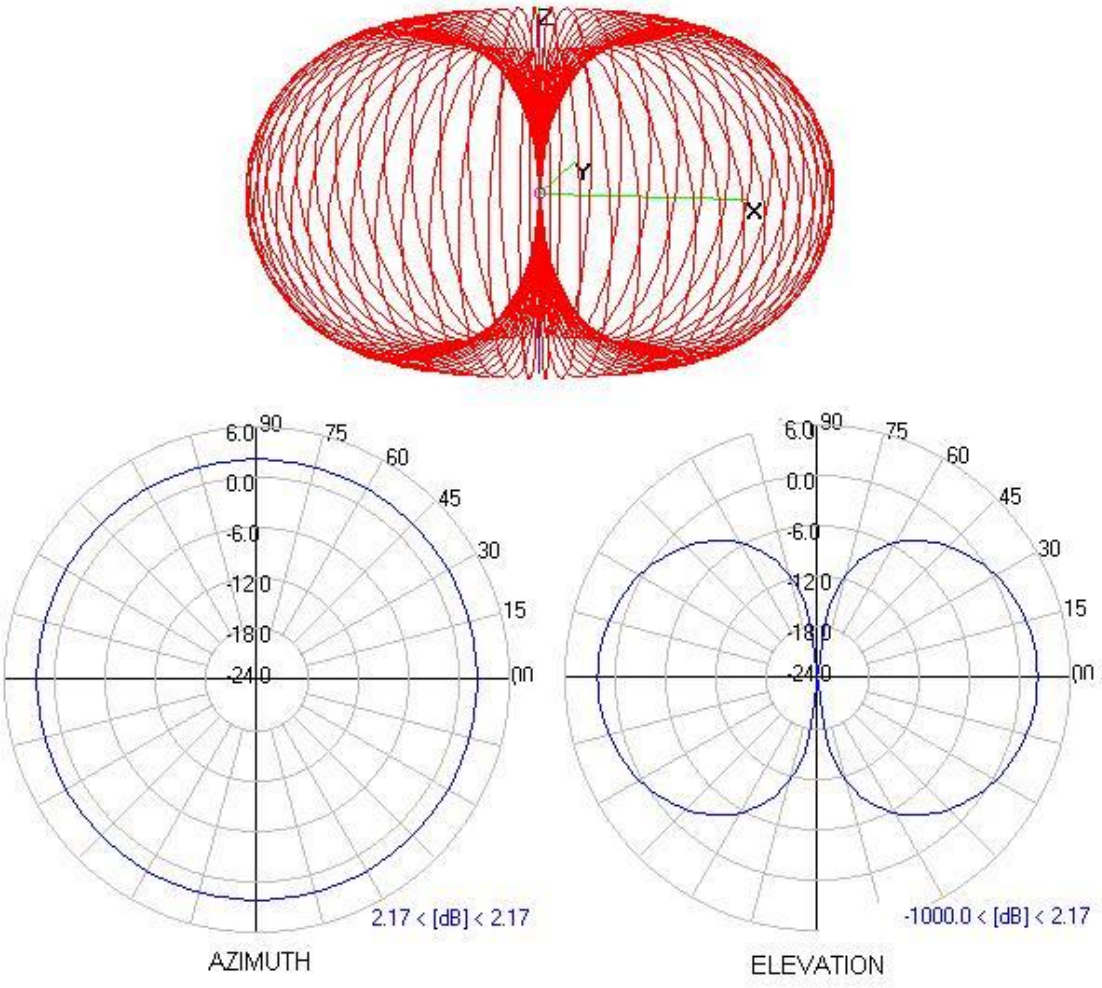


Figura 5-6 Radiación de una antena Omnidireccional

Los fabricantes de antenas proporcionan los gráficos de emisión de las mismas en dos diagramas llamados “Azimuth” y “Elevación”, como se ven en la figura anterior. Azmuth es el patrón de radiación de la antena visto desde arriba y lo que nos dice es cómo se propaga la señal en el plano horizontal. La elevación sería la forma en que se propaga hacia arriba y hacia abajo. Si la antena radia en todas direcciones de igual forma se dice que es una “Radiación Isotrópica”. Una antena Omnidireccional instalada en un piso radiará la mayor parte de su energía en el plano horizontal de dicho piso, aunque también se irradiará una fracción de su señal a los pisos superiores e inferiores.

La ganancia:

La ganancia es un concepto complejo pero necesario para entender el funcionamiento de las antenas. Formalmente se define de la siguiente manera:

"La ganancia de una antena se define como la relación entre la densidad de potencia radiada en una dirección y la densidad de potencia que radiaría una antena isotrópica, a igualdad de distancias y potencias entregadas a la antena".

Es una medida logarítmica y se expresa en "dBi". Realmente, la ganancia indica la potencia que una antena gana en una dirección específica si la comparáramos con una antena isotrópica que tendría ganancia igual a 0. Por eso se llama ganancia, ya que mide la potencia ganada en esa dirección.

"A mayor ganancia mayor potencia".

La ganancia típica de las antenas que se incluyen en los puntos de acceso es de 2dBi aproximadamente. Esto es normal. Por definición si una antena radia mucho en una dirección, tiene que radiar poco en otras. Es por eso que una antena omnidireccional suele tener poca ganancia y es muy difícil encontrar antenas con ganancias superiores a los 8dBi.

Antenas direccionales:

Las antenas direccionales, como su nombre indica radian la mayor parte de su energía en una dirección concreta. De ese modo el patrón de radiación de una antena direccional es algo parecido a un lóbulo. (Véase Figura 5-7)

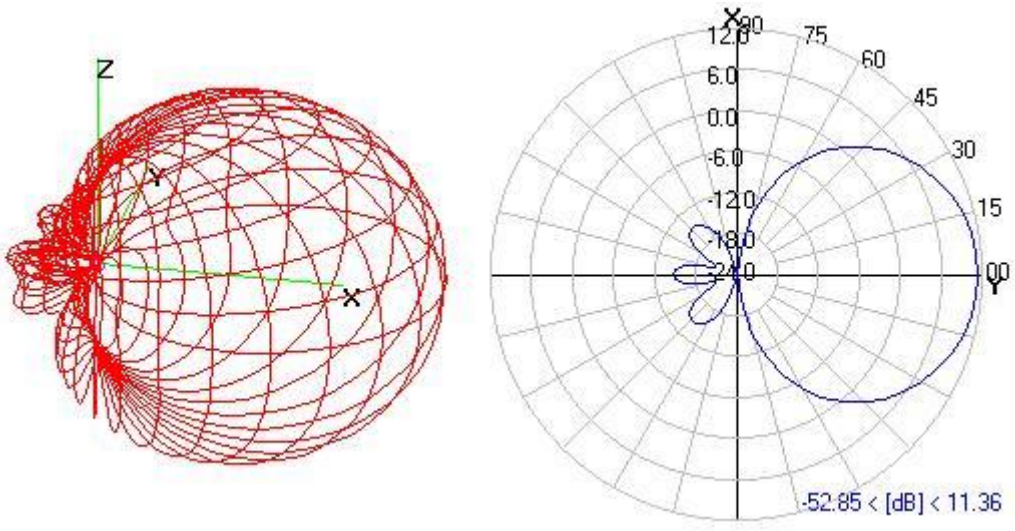


Figura 5-7 Radiación de una antena Direccional

Como característica principal tiene que en el plano horizontal y vertical es prácticamente idéntico, por lo que sólo se suele mostrar un único gráfico en lugar de los dos que se muestran en las Omnidireccionales. Por la propia definición de Ganancia, es fácil prever que en el caso de las antenas Direccionales, este parámetro será mayor que con las Omnidireccionales.

Selección de una antena

La selección de una antena depende primero del tipo de cobertura que queramos dar. Hacia todas direcciones o hacia una dirección concreta. A mayor ganancia, mayores distancias obtenidas. Es necesario resaltar que las antenas direccionales obtienen mayor ganancia "achatando" el lóbulo de emisión, lo que implica que a mayor ganancia, mejor distancia pero menor ángulo de apertura.

Existe una gran diversidad de tipos de antena, dependiendo del uso a que van a ser destinadas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas (ejemplo: una emisora de radio o la central de los teléfonos celulares), otras veces deben serlo para canalizar la potencia y no interferir a otros servicios (antenas entre estaciones de radioenlaces). También es una antena la ferrita que permite oír un radio-receptor a transistores, o la que está integrada en la computadora portátil para conectarse a las redes Wi-Fi.

Todos los equipos Wi-Fi ya incorporan sus propias antenas. No obstante, cuando se desea disponer de una red de mayor alcance o cobertura, a veces, resulta conveniente sustituir la antena incorporada en el equipo Wi-Fi por otra exterior con mayor ganancia.

La razón para que no existan reglas absolutas para el diseño y localización de antenas es que son muchas variables las que afectan la propagación de la señal electromagnética. Además, con las redes inalámbricas nos enfrentamos a usuarios móviles y condiciones ambientales cambiantes.

La mayoría de las antenas que incorporan los equipos Wi-Fi son antenas internas. Esto quiere decir que son antenas que vienen incluidas dentro de la unidad del AP o del adaptador de red (tarjeta PCMCIA o dispositivo USB). Las antenas internas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tiene el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos Puntos de Acceso, la mejor solución es instalar una antena externa. Con una buena antena externa, la señal Wi-Fi de un Punto de Acceso puede llegar a superar los 15 kilómetros de alcance siempre y cuando no haya obstáculos, como edificios o árboles y que la antena este bien colocada.

Para el caso exclusivo de la red inalámbrica del Instituto de Física, no se contemplo la instalación de antenas externas porque representaría un mayor gasto en el proyecto al no aprovechar la infraestructura cableada ya existente. Además de que se desea limitar la cobertura al interior del Instituto de Física, por cuestiones de seguridad y de convivencia con la RIU (Red Inalámbrica Universitaria) que provee la conexión a internet sin cables en áreas comunes de Ciudad Universitaria de manera exclusiva a los alumnos inscritos, y personal académico y administrativo que así lo soliciten.

Dispositivos Handheld

Como su nombre indica, estamos hablando de un PC de Mano. Básicamente se trata de verdaderas computadoras de bolsillo que permiten, estés donde estés, llevar contigo tus datos más importantes. ¿PocketPC o Handheld PC?

La diferencia más llamativa entre estos dispositivos, es la incorporación de un teclado QWERTY y una pantalla táctil de 640x240 píxeles frente a los 240x320 de una Pocket PC. Debido a estos 2 factores, el peso de una Handheld PC será más elevado que el de una PocketPC. Por todo lo demás, son dispositivos muy parecidos basados en una plataforma cómun, Microsoft WindowsCE.

Desde que las Handheld PC hicieron su aparición en el mercado, Hewlet Packard fue y sigue siendo el mejor aliado de estos dispositivos, apostando fuertemente con sus H/PC Jornada. La Serie 700 de HP y junto a sus hermanas la 710 y 728 han marcado un mito dentro de las computadoras de bolsillo. Aunque otros fabricantes también apostaron por la plataforma Handheld como son Nec o Siemens.

4.8. Seguridad en las Redes Inalámbricas

No existe ningún sistema de seguridad que sea absolutamente impenetrable. Como se sabe, el objetivo de cualquier sistema de seguridad es permitir el acceso a cualquier persona autorizada e impedírselo a cualquier otra. Sin embargo, el simple hecho de que una persona puede entrar, aunque sea de forma autorizada, hace que el sistema deje de ser impenetrable. Si un intruso puede averiguar los pasos a dar para entrar legalmente, conseguirá romper la barrera.

Las comunicaciones inalámbricas tiene un inconveniente particular: carece de barreras físicas. Por tanto, cualquier persona, con unos conocimientos mínimos sobre seguridad y con una tarjeta Wi-Fi instalada en la PC puede, potencialmente, acceder a un Punto de Acceso de una red inalámbrica. No obstante, fundamentalmente, lo que hace esto sea cierto es que muy pocos usuarios se toman en serio las medidas de seguridad. Por ejemplo, suele ser común que el usuario instale una red inalámbrica sin modificar la configuración que trae el sistema por defecto. Si un intruso desea entrar en un sistema, lo primero que comprobará es si todavía tiene la configuración inicial.

Por tanto, independientemente de las redes inalámbricas sean más o menos seguras, lo que sí es cierto es que vienen provistas de medidas de seguridad para evitar que personas ajenas puedan hacer uso de la red. Estas medidas son lo suficientemente buenas como para la inmensa mayoría de las personas que tenemos a nuestro alrededor no puedan entrar en la red.

Aparte de lo anterior, es cierto que la seguridad del sistema Wi-Fi no es de las mejores. Se le ha criticado extensivamente de ser un sistema muy débil, hasta el punto que IEEE ha creado un grupo de trabajo (802.11i) con el objetivo de proponer las medidas necesarias para conseguir un sistema Wi-Fi completamente seguro.

Difusión del nombre de la Red

SSID (Service Set Identifier, 'Identificador del conjunto de servicios') es un código alfanumérico que se configura en cada computadora y AP que formen parte de la WLAN. Este código puede ser utilizado como una simple contraseña entre la estación y el AP o como un identificador del equipo emisor en una red pública. Existen APs que permiten que se les deshabilite el sistema SSID.

Este sistema no garantiza la seguridad, ya que los códigos SSID son emitidos en forma de texto sin codificar. Cualquier receptor con el software adecuado puede averiguar estos datos. De hecho, Windows XP, Windows Vista, y algunos dispositivos portátiles de entretenimiento (PSP, NDS, etc.) incluyen algún programa capaz de detectar automáticamente estos códigos y mostrarle al usuario la lista de redes (listas SSID) detectadas para que el usuario elija a cual desea conectarse.

Bloqueo de direcciones MAC

Se puede generar una lista de direcciones MAC y limitar el acceso a la red a aquellos usuarios contemplados en la lista. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo 12-AB-45-67-89-CD) e identifican a la tarjeta de los adaptadores de red. Las direcciones MAC no son modificables por el usuario. No obstante, es cierto que estas direcciones se transmiten en forma de texto sin codificar y por lo tanto, son fácilmente detectadas con un receptor adecuado. Un intruso experimentado podría leer una dirección correcta, configurarla en otra estación y acceder sin problemas.

4.9 Protocolos de seguridad para redes inalámbricas.

WEP

Para solucionar los problemas de seguridad de transferencia en redes inalámbricas, el estándar 802.11 incluye un sencillo mecanismo de cifrado llamado WEP (Privacidad equivalente al cableado).

Con este sistema se cifran todos los datos que se intercambian entre las computadoras y los AP. WEP utiliza el algoritmo de cifrado PRGN (Pseudorandom Number Generation, 'Generación de Números Pseudoaleatorios') RC4 desarrollado en 1987 por RSA Data Security.
La utilización de la técnica del cifrado WEP es opcional.

WEP es un protocolo de cifrado de trama de datos 802.11 que utiliza el algoritmo simétrico RC4 con claves de 64 bits o 128 bits. El concepto de WEP consiste en establecer una clave secreta de 40 ó 128 bits con anticipación. Esta clave secreta se debe declarar tanto en el punto de acceso como en los equipos cliente. La clave se usa para crear un número que parece aleatorio y de la misma longitud que la trama de datos. Cada transmisión de datos se cifra de la siguiente manera. Al utilizar el

número que parece aleatorio como una "máscara", se usa una operación "X-OR" para combinar la trama y el número que parece aleatorio en un flujo de datos cifrado.

La clave de sesión que comparten todas las estaciones es estática, es decir que para poner en funcionamiento un número elevado de estaciones inalámbricas, éstas deben configurarse con la misma clave de sesión. Por lo tanto, con sólo saber la clave se pueden descifrar las señales.

Debilidades de WEP

Para la inicialización se usan sólo 24 bits de la clave, lo que implica que sólo 40 de 64 bits o 104 de 128 bits de la clave se utilizan realmente para el cifrado.

En el caso de una clave de 40 bits, con un ataque de fuerza bruta (que prueba todas las claves posibles) un hacker puede encontrar la clave de sesión con rapidez. Asimismo, una falla detectada en la generación del flujo que parece aleatorio permite que se descubra la clave de sesión al almacenar y analizar de 100 MB a 1 GB de tráfico.

Por lo tanto, el WEP no es suficiente para garantizar verdaderamente la privacidad de los datos. Sin embargo, se recomienda utilizar al menos una clave WEP de 128 bits para garantizar un nivel de privacidad mínimo. Esto puede reducir el riesgo de una intrusión en un 90 por ciento

WPA

WPA es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WPA utiliza TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 802.1X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits.

La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

WPA-PSK

Es el sistema más simple de control de acceso después de WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad.

PSK (PreShared Key, Clave compartida Previamente), basa su seguridad en una contraseña compartida. WPA-PSK usa una clave compartida de acceso de una longitud entre 8 y 63 caracteres. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes inalámbricas. Su configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

Debilidades de WPA-PSK

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir, ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería representar mayores problemas.

Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

4.9.1 RIESGOS

La seguridad es un riesgo tanto para las redes inalámbricas como para las cableadas. Hasta la fecha, todas las tecnologías informáticas que han ido apareciendo en el mercado (desde la PC hasta las redes de cualquier tipo), han sido susceptibles, de una u otra forma, de ser violadas en su integridad, confidencialidad o autenticidad de los datos que contiene.

Ciertamente, a diferencia de las redes cableadas, las redes inalámbricas emiten señales que pueden ser fácilmente recogidas en el exterior del sitio vigilado de la red (la oficina, escuela o el hogar particular). Desde ese punto de vista, las redes inalámbricas tienen un riesgo añadido. Pero este riesgo es controlable. De la misma forma que es controlable el riesgo que tiene una red cableada de que un usuario remoto y desconocido pueda entrar a ella a través de su conexión de Internet. El riesgo siempre existe si no se toman las precauciones necesarias.

Las cuatro categorías de riesgos que preocupan en el uso de cualquier tecnología de red son:

Pérdida del equipo

A veces es sorprendente la cantidad de información que podemos llegar a almacenar en un disco duro, información no sólo profesional, sino incluso, personal. Perder un equipo puede convertirse en un gran problema si llega a caer en manos equivocadas.

A parte del problema que supone el exponer determinada información a usuarios no autorizados, existe un problema adicional y es que dicho equipo podría ser utilizado para acceder a la red de una empresa. Este problema existe tanto si la computadora está conectada a una red cableada como si lo está a una red inalámbrica.

Si la red es cableada, el acceso a la red se podría hacer desde cualquier parte del mundo vía internet (si tiene las claves grabadas). En este caso, este riesgo puede eliminarse fácilmente al deshabilitar las cuentas de acceso del usuario en cuestión.

Si la red es inalámbrica, el acceso se tendría que hacer necesariamente desde una zona de cobertura. En este caso, pueden cambiarse también todos los códigos de acceso. No obstante, es cierto que, administrativamente, es mucho más sencillo eliminar una cuanta de acceso de una red cableada que cambiar manualmente las configuraciones de acceso de todos los usuarios de la red inalámbrica. Sin embargo, también es cierto que, a menos que exista algún tipo de etiqueta

identificativa, la persona que consiga dicho equipo puede no disponer de ninguna pista para saber donde se encuentra la red inalámbrica a la que se accede desde el equipo.

Infección por virus

Los virus son pequeños programas informáticos que pueden directamente producir daño en la computadora o ser utilizados para conseguir otros fines haciendo uso de la red o el equipo donde se alojan. Los virus afectan tanto a redes cableadas como inalámbricas.

Esto quiere decir que las medidas antivirus son idénticas para cualquier tipo de red, debemos mantener el programa antivirus actualizado y disponer de un firewall.

Uso equivocado por personas no autorizadas

El hacer un mal uso del sistema (intencionado o accidental) por personas autorizadas a utilizarlo es una amenaza de la que es difícil protegerse. Una vez que el usuario ha pasado todos los niveles de seguridad y se encuentra dentro del sistema, es complicado controlar en detalle el uso que cada usuario hace de él.

Existen los casos de empleados que han robado información de la empresa donde trabajan, borrado archivos, modificado información sensible o hecho cualquier otro uso malintencionado de la información. También existen los casos que si ninguna intención de afectar al sistema, logran daños considerables de manera accidental. Y todos estos riesgos son equivalentes tanto para redes cableadas como para redes inalámbricas.

Solo estableciendo políticas de seguridad adecuadas, y hacer seguimientos periódicos de su cumplimiento, nos ayudará a disminuir riesgos para la red.

Uso fraudulento por personas no autorizadas

Si hay un punto en el que las WLAN tienen desventaja frente a las LAN, ése es el riesgo de uso fraudulento por personas no autorizadas. La desventaja viene por lo que es su ventaja fundamental: cualquier usuario puede conectarse a la red desde cualquier sitio sin necesidad de conectarse físicamente a algún medio.

Los usos fraudulentos pueden venir por cualquiera de los siguientes caminos:

- Escuchar: con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por terceras personas. De hecho, existen programas como Airopeek, Airsnort, NetStumbler o Wepcrack que facilitan esta labor. Estos programas descubren datos como el SSID (Service Set Identifier), la dirección MAC o si el sistema WEP está o no habilitado.

- Acceder: Se trata de configurar un dispositivo para acceder a una red para la que no se tiene autorización. Esto se puede hacer de dos formas: configurando una estación para que acceda a un punto de acceso existente o instalando un nuevo punto de acceso y, a través de él, conectar fraudulentamente todos los equipos externos que se deseen.

- Romper la Clave: Consiste en intentar adivinar la clave de acceso de un usuario autorizado mediante intentos sucesivos.

- Saturar: en este caso no se trata de intentar acceder fraudulentamente a una red, sino de dejarla fuera de servicio. El resultado es que la red no puede ser utilizada por sus propios usuarios, por lo que es un ataque a la seguridad. Para dejar inhabilitada una WLAN, bastaría simplemente con saturar el medio radioeléctrico con el suficiente ruido como para que sea imposible llevar a cabo cualquier comunicación. A este tipo de ataques se les conoce también como obstrucción de servicio, DOS (Denial of Service) o jamming (atasco).

5

Desarrollo de la Red inalámbrica en el IFUNAM.

5.1 Hipótesis

La implementación de una WLAN en el instituto de Física, ayudara a resolver el problema de saturación de usuarios en la red cableada y el problema de las direcciones IP. Se tendrá un acceso más fácil y sin las limitantes que el cable implica. Así como la reducción de costos de mantenimiento y el acceso a la red en lugares donde antes no existía el servicio.

5.2. Objetivos

- Aplicar los conocimientos en redes y cómputo adquiridos en la carrera de Ingeniería en Computación y la experiencia laboral.
- Diseñar la red inalámbrica del IFUNAM de acuerdo a las necesidades de la institución.
- Implementar la red inalámbrica del IFUNAM.
- Implementar la seguridad de la red inalámbrica
- Implementar la administración y monitoreo del tráfico de la red
- Dar un uso más eficiente al rango de direcciones IP

5.3. Descripción de las instalaciones

El instituto de Física de la Universidad Nacional Autónoma de México (IFUNAM) es uno de los centros de investigación en Física más importante del país, el IFUNAM se encuentra localizado en Ciudad Universitaria. Cuenta con 6 edificios (figura 3-1): edificio principal, biblioteca, taller mecánico, edificio de aceleradores, acelerador Van de Graff 5.5 y edificio Colisur, en los cuales se encuentran los cubículos de investigadores, académicos, administrativos, biblioteca, auditorio, acelerador peletrón, acelerador 0.7 MeV, acelerador 2 MeV y el laboratorio central de microscopia electrónica.

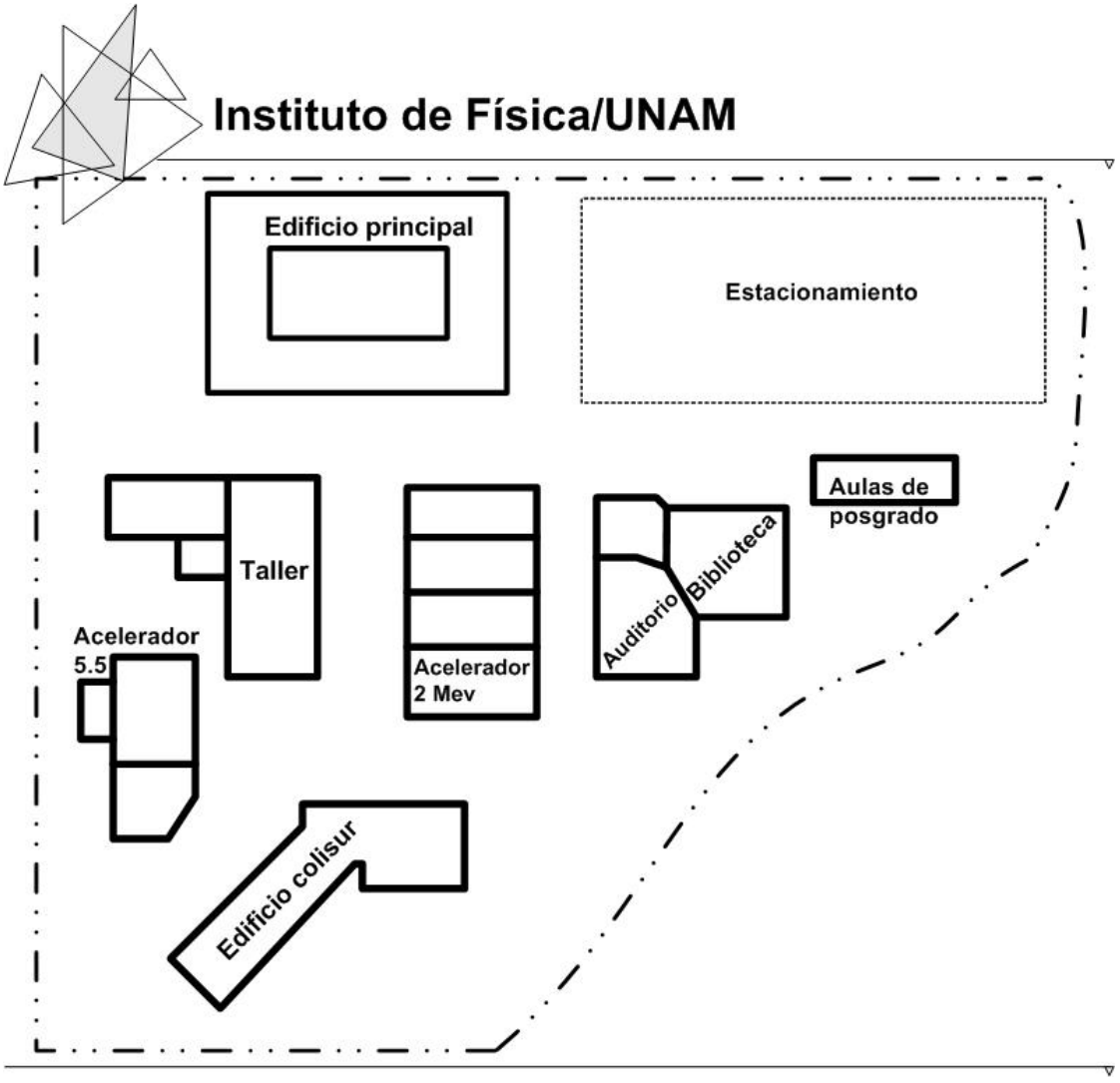


Figura 5-1 Ubicación de las instalaciones del IFUNAM

Ubicación	Perímetro (m)	Área (m^2)
Instituto de Física	732.9	32,398.5
Edificio Principal	224.0	3,013.0
Colisur	181.6	1,086.4
Taller	179.3	1,329.0
Acelerador 5.5	135.5	791.2
Acelerador 2 Mev	154.0	1,353.0
Auditorio	86.6	489.2
Biblioteca	78.7	406.6
Aulas de Posgrado	74.0	260.0
Estacionamiento	249.2	3,782.0

Tabla 5-1 Dimensiones de los edificios de las instalaciones del instituto de Física

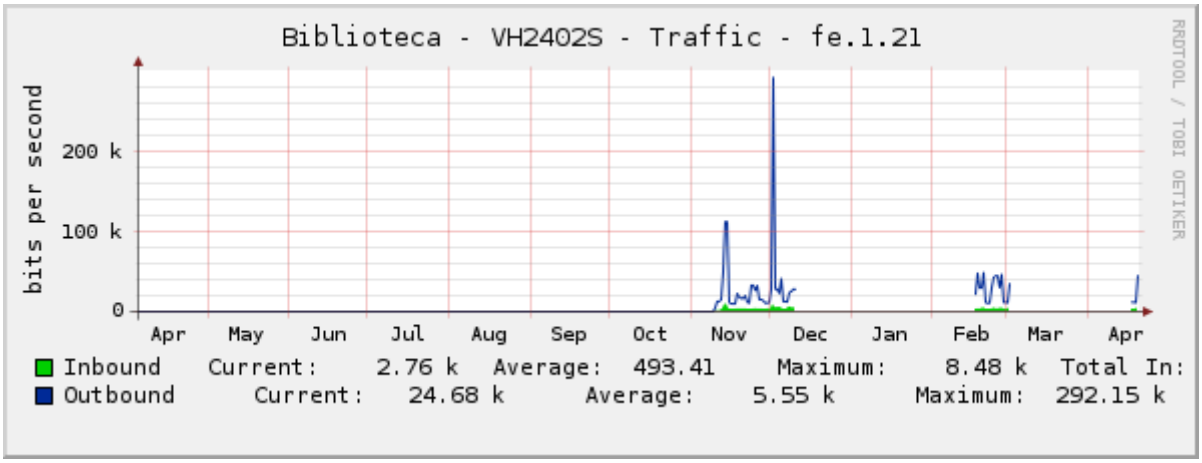
En general todos los espacios descritos anteriormente cuentan con conexión a la red local mediante cableado estructurado y el objeto de estudio se centra en la posibilidad de instalar una red inalámbrica que permita resolver la demanda de conectividad a la red y movilidad de los usuarios.

Red Inalámbrica Universitaria (RIU)

La Red Inalámbrica Universitaria proporciona el servicio de conexión a Internet a los dispositivos móviles como LapTops, Palm, entre otros, y su cobertura está limitada a las escuelas, facultades, institutos y centros de investigación, bibliotecas, recintos culturales y áreas de congregación de estudiantes e investigadores universitarios en la Ciudad Universitaria e irá creciendo conforme la demanda lo solicite.

Cobertura de la RIU en el Instituto de Física

La cobertura de la RIU en el Instituto está limitada debido a que solo tenemos 2 puntos de acceso instalados, el primero en la biblioteca “Juan B. de Oyarzábal”, y el segundo punto de acceso se encuentra en el auditorio “Alejandra Jáidar”. De esta forma en nuestras instalaciones no tenemos conocimiento de la densidad de usuarios que hagan uso de la RIU. La figura 5-2 muestra el uso de ancho de banda que demanda el punto de acceso de la RIU que está instalado en la biblioteca “Juan B. de Oyarzábal”, esta grafica se toma del switch de red a donde está conectado el punto de acceso.



5-2 Ancho de banda del AP de la RIU

Canales de radiofrecuencia de la RIU

En temas anteriores comentamos acerca de la distribución de los canales de radio frecuencia y el posible solapamiento que ocurriría si no configuramos correctamente los puntos de acceso. Para que los equipos de nuestra red puedan convivir con los equipos de la RIU se realizo el escaneo de la señal usando el Sniffer NetStumbler para verificar los canales de radiofrecuencia en los cuales están emitiendo la señal los equipos de la RIU y así configurar diferentes canales a nuestros puntos de acceso de manera que ambas redes convivan sin ningún tipo de conflicto.

El Primer Punto de acceso de la RIU, como anteriormente lo mencionamos, se encuentra en el primer piso de la biblioteca “Juan B. de Oyarzábal”, y se encuentra configurado en el canal “1” y el segundo punto de acceso se encuentra en la planta baja dentro del auditorio “Alejandra Jáidar” el cual trabaja en el canal “6”, por lo tanto para evitar colisiones, el AP del IFUNAM ubicado en el primer piso lo configuramos en el canal “6” y el de la planta baja queda funcionando en el canal “11” y de esta manera ambas redes puedes convivir de manera transparente.

5.4. Diseño de la Red Inalámbrica

Para el diseño de la Red inalámbrica se tomaron en cuenta los siguientes puntos, dado que son importantes para la correcta operación de la Red.

5.4.1. Dispositivos de la Red Inalámbrica

Punto de acceso inalámbrico

Existen multitud de fabricantes, y cada uno de ellos proporciona características básicas u otras más avanzadas a sus equipos como valor agregado:

- Firewall integrado.
- Switch 4 puertos incorporado.
- Función de bridge entre edificios.
- Función de repetidor.
- Potencia de emisión variable.
- DHCP, etc.

Para que realicen su función estos usan un canal de frecuencia donde emitirán la señal, esta frecuencia es configurable por el usuario. De esta manera cualquier dispositivo cliente Wireless detectará que en ese canal existe un AP e intentará conectarse con él siempre que:

- El usuario conozca el Identificador del Canal (SSID).
- No sea un canal cifrado.
- No requiera autentificación con login y contraseña.

En resumen, nos podremos conectar con un AP que no tenga ningún tipo de filtrado ni autentificación.

La mayoría de los puntos de acceso del mercado proporcionan un servidor de DHCP para que asigne automáticamente direcciones IPs a los equipos que se conectan, de esta manera el usuario no tiene que conocer los datos técnicos de la conexión a la red, es decir, es transparente al usuario. La dirección de la puerta de enlace (gateway) y de los servidores de nombres de dominio (DNS) también se proporciona para que el host cliente esté completamente configurado y funcionando.

Existen otros dispositivos como son: servidores de impresión inalámbricos, o las cámaras inalámbricas, pero solamente son aplicaciones inalámbricas, no son dispositivos que permitan crear redes WLAN.

5.4.2. Topologías de la Red Inalámbrica

Las redes inalámbricas pueden construirse sin o con Punto de Acceso (AP), esto es lo que nos determina si es "Ad-Hoc" o "Infraestructura".

Ad Hoc

Red igual a igual (peer to peer).

Al igual que las redes cableadas Ethernet, en las cuales compartimos el medio (cable) y se pueden realizar varias "conexiones" a la vez entre distintos Host, el medio de las redes WLAN (aire) dispone de un identificador único para cada una de esas "conexiones" simultaneas que se pueden realizar, este identificador es una dirección MAC (48 bits).

En el caso de las redes Ad-Hoc, este número MAC es generado por el adaptador inalámbrico que crea "la conexión", y es un identificador MAC aleatorio.

Cuando un adaptador Wireless es activado, primero pasa a un estado de "escucha", en el cual, durante unos 6 segundos está buscando por todos los canales alguna "conexión" activa. Si encuentra alguno, le indicará al usuario a cual se quiere conectar.

En el supuesto de que no se pueda conectar a otro Host que ya estuviera activo, pasa a "crear la conexión", para que otros equipos se puedan conectar a él.

Para una determinada WLAN con topología Adhoc, todos los equipos conectados a ella (Host) deben de ser configurados con el mismo Identificador de Servicio Básico (Basic Service Set, BSSID).

El modo Ad-hoc como máximo puede soportar 256 usuarios, pero es algo inviable ya que sería una red inalámbrica que no funcionará correctamente. Cuando se necesita un número elevado de usuarios debemos de utilizar una topología

Infraestructura

Del mismo modo, como en las redes Ethernet, en las cuales se dispone de un Hub o switch para "unir" todos los Host, ahora disponemos de los Puntos de Acceso (AP), los cuales se encargan de "crear las conexiones" para que se puedan conectar el resto de Host inalámbricos que están dentro de su área de cobertura.

Ahora la MAC que identifica a esta "conexión" es la MAC del AP (MAC real wireless), un dato que puede ser observado con cualquier programa Sniffer Wireless.

Una configuración en Infraestructura debe configurarse como un Extended Service Set (ESSID). Los usuarios con el mismo ESSID se pueden desplazar libremente entre varios APs mientras el servicio continua (roaming).

El modo Infraestructura, como máximo puede soportar 2048 usuarios, pero al igual que en el caso Ad-hoc es inviable el montar una red con un número tan alto de usuarios sobre el mismo AP.

Dependiendo del tipo de uso del ancho de banda que se necesite, se estudiará el número de AP necesarios para conseguir una total cobertura del edificio, teniendo en cuenta otros factores como la redundancia ante la caída de uno de los APs, para que esa zona este también cubierta por otro próximo. Un tema cada vez más importante en las redes donde la disponibilidad tiene que ser de 7x24.

5.4.3. Cobertura de la Red inalámbrica

Roaming

Unas de las utilidades más interesantes de esta tecnología inalámbrica, es la posibilidad de realizar roaming entre los APs del Instituto, con lo que al igual que la tecnología celular, no perdemos cobertura y podemos movernos desde el área de cobertura de un AP a otro sin problemas, para ello debemos configurar los APs para que trabajen en distintos canales de frecuencia para que no se produzcan problemas de funcionamiento / interferencias en las zonas donde existe cobertura de más de un AP. (Véase Figura 5-2)

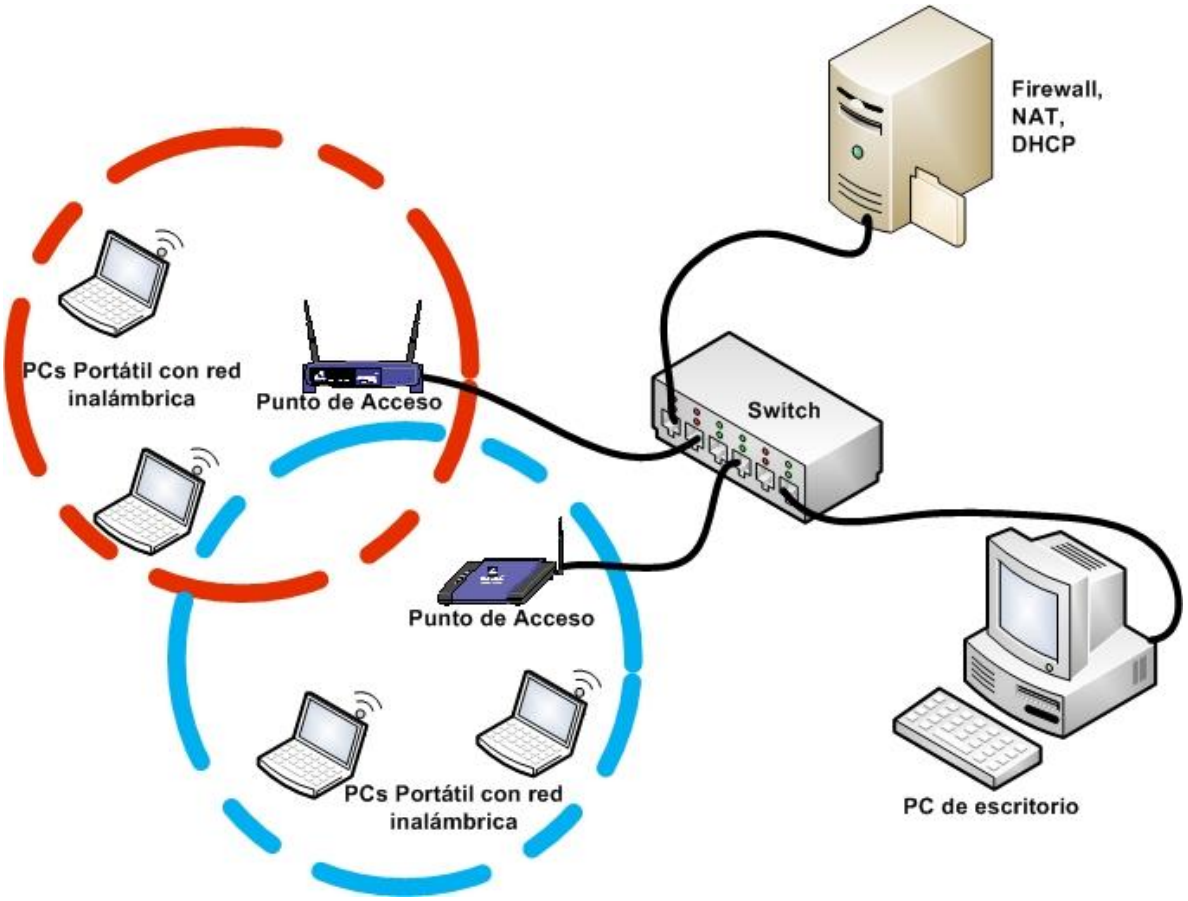


Figura 5-2 Red inalámbrica con Roaming

Solapamiento de canales

Como ya comentamos anteriormente, cada uno de los 11 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 Mhz, y la gama de frecuencias disponible va de los 2.412 GHz hasta los 2.484 GHz. En este espacio está dividido en 11 canales, solapándose los canales adyacentes.

Como resultado solo tenemos las siguientes combinaciones de canales enteros (1,6 y 11) en los que colocar los puntos de acceso para que no se hagan interferencias entre ellos, en caso de que necesitemos más canales utilizaremos el mínimo solapamiento. (Véase Figura 5-3)

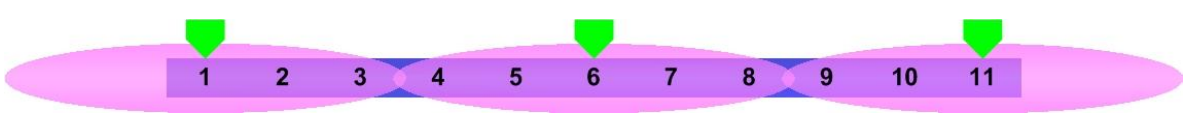


Figura 5-3 Solapamiento de canales 2.4 Ghz

5.4.4. Seguridad de la Red Inalámbrica

La seguridad es uno de los temas más discutidos en el tema de las redes inalámbricas. El disponer de una red inalámbrica significa que se deben de tomar LAS MISMAS MEDIDAS como en una red cableada:

- Autentificar las conexiones con login y password.
- No compartir recursos innecesarios en la red.
- Poner restricciones a los elementos críticos de la red, tal como servidores de aplicaciones, servidores de archivos, servidores web, etc.

Si contamos con una WLAN en nuestro lugar de trabajo, se deben de tomar una serie de medidas de prevención como son:

- Realizar escaneos buscando posibles Puntos de Acceso no autorizados por el personal de informática.

Existen herramientas potentes para hacer escaneos, en este caso usamos NetStumbler, que nos ayuda a detectar puntos de acceso no autorizados y de esta forma poder establecer los sistemas o mecanismos de protección básicos a nuestra red inalámbrica.

Sniffer NetStumbler

Uno de los sniffers más conocidos de la red, principalmente porque funciona bajo Windows y es de muy fácil uso. No es el mejor, pero sí el más usado lo que hace que sea una de las herramientas más comunes de los usuarios inalámbricos.

Nosotros la utilizamos para comprobar la cobertura de nuestra red, las ganancias de las antenas, verificar cuántos APs están operando correctamente, etc. En resumen, es una herramienta que tiene lo que necesita cualquier técnico o administrador de red para obtener información sobre los dispositivos que conforman la red inalámbrica. (Véase Figura 5-4)

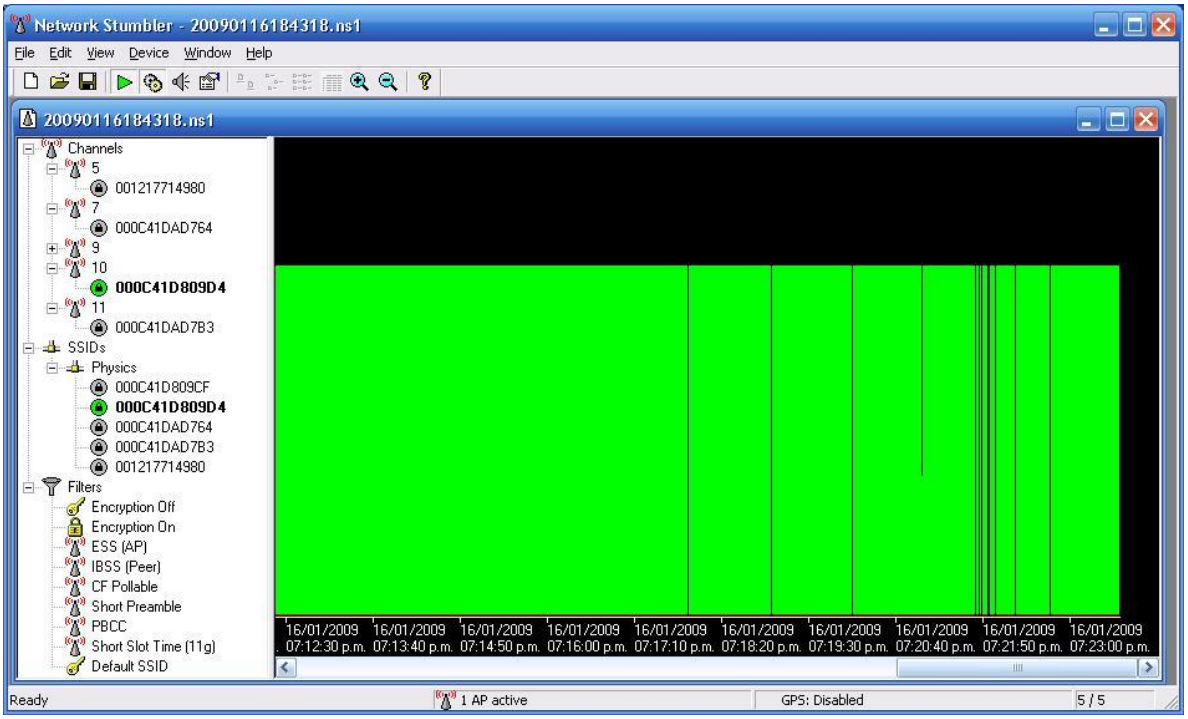


Figura 5-4 Sniffer NetStumbler

Filtrado por direcciones MAC

Este tipo de seguridad lo proporciona cualquier Punto de Acceso. Es un sistema muy básico pero también efectivo, aunque es vulnerable.

Podemos configurar el AP para que permita o impida el acceso a determinadas MACs, y ya sabemos que “oficialmente” no pueden existir dos tarjetas con la misma MAC.

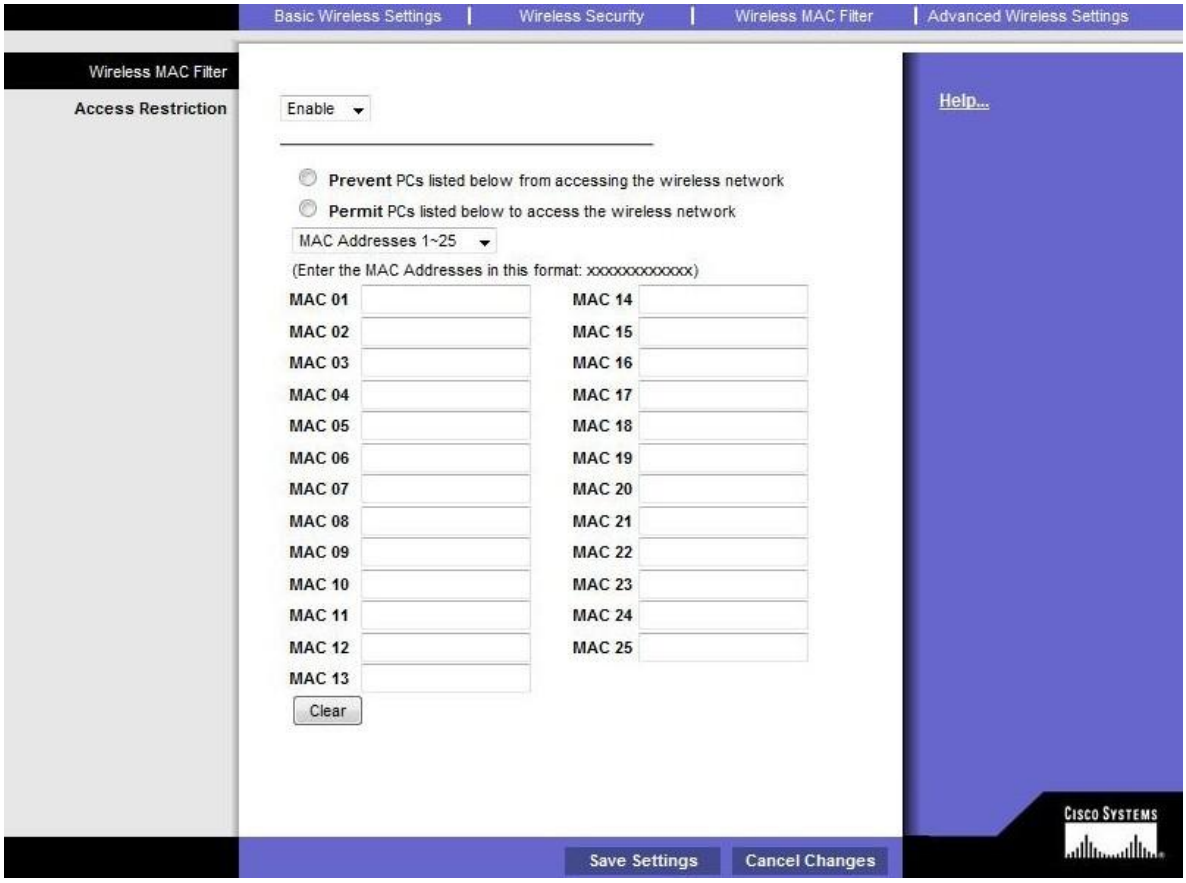


Figura 5-5 Filtrado de direcciones MAC

Para nuestro proyecto, el bloqueo de direcciones MAC se hace a través del firewall, que usa Sistema Operativo OpenBSD y tiene configurado los siguientes servicios:

- **Firewall**: Se usa pf (*packet filter*) para permitir o negar accesos a sitios web y también para bloquear el tráfico de una PC en particular bloqueando su dirección IP o su dirección MAC.
- **Servidor DHCP**: Se ocupa para asignar el direccionamiento IP de forma automática en la Red Inalámbrica.
- **Servidor NAT**: Para que los equipos PCs puedan acceder a Internet mediante el uso de un rango de IPs privadas.

Difusión del Nombre de la Red

Definido en el 802.11, el procedimiento SSID (Service Set Identifier) incluye un identificador único en la cabecera de los mensajes que actúa como contraseña cuando un dispositivo quiere conectarse al sistema.

Un sniffer puede capturar la información SSID en alguna trama aunque su difusión esté desactivada, esto incorpora poca seguridad, pero al igual que el bloqueo de MACS es una característica que se debe establecer.

Para desactivar la difusión del SSID en el AP, lo tenemos hacer desde la configuración del AP en Broadcast SSID. (Véase Figura 5-6)

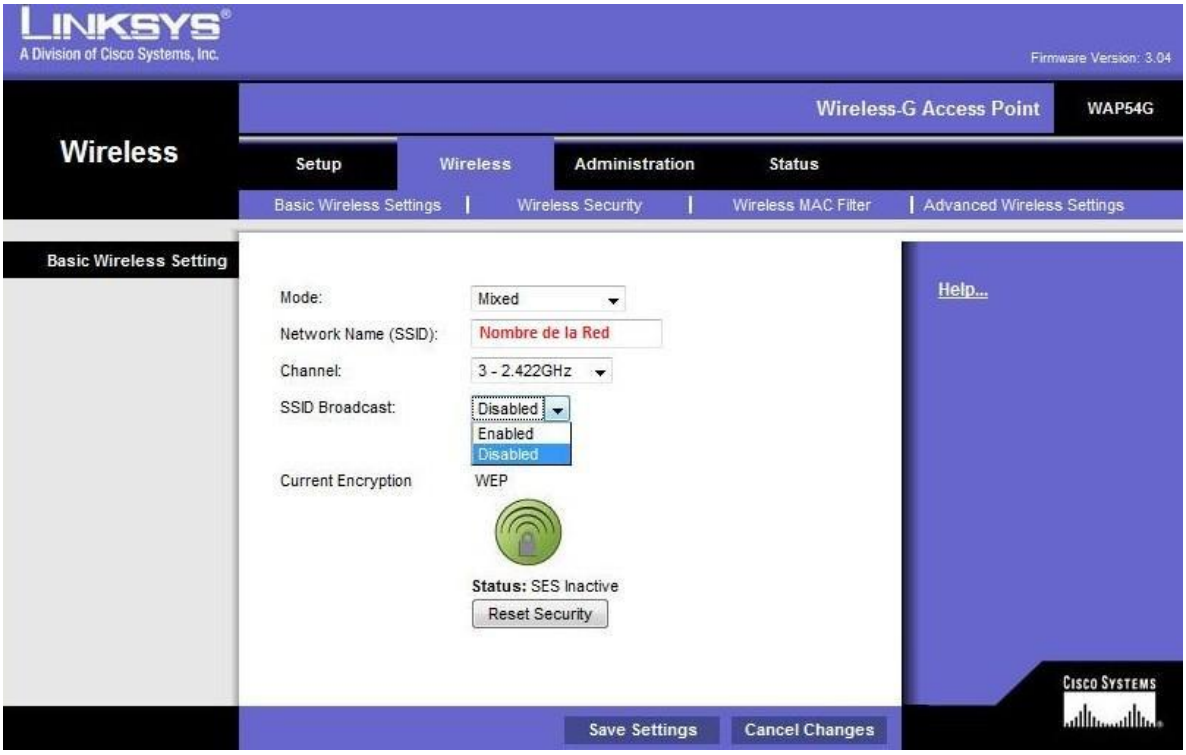


Figura 5-6 Difusión del nombre de la red bloqueada

Uso de protocolos de encriptación WEP

Wired Equivalent Privacy, Privacidad equivalente a redes cableadas. Utiliza un algoritmo de encriptación RC4, y claves de cifrado de 64, 128 y 256 bits; pero en realidad las utiliza de 40, 104 y 152 respectivamente, el resto (overhead), no es información significativa para el cifrado.

Nota: WEP de 256 bits no es estándar y no todos los dispositivos lo aceptan.

Actualmente esta implementado en todos los sistemas (APs, routers inalámbricos) y normalmente son compatibles, pero si es necesario asegurar que los equipos cuenten con esta característica.

Utiliza una clave de cifrado asignada por el administrador tanto a las PCs como a los puntos de acceso. El cifrado es simétrico tanto para cifrado como para descifrado, por lo que para alcanzar un nivel aceptable de seguridad las claves deben ser cambiadas con frecuencia en todos los dispositivos por el administrador, por ello WEP tiene los días contados y han surgido otros protocolos de encriptación mucho mejores como el WAP.(Figura 5-7)

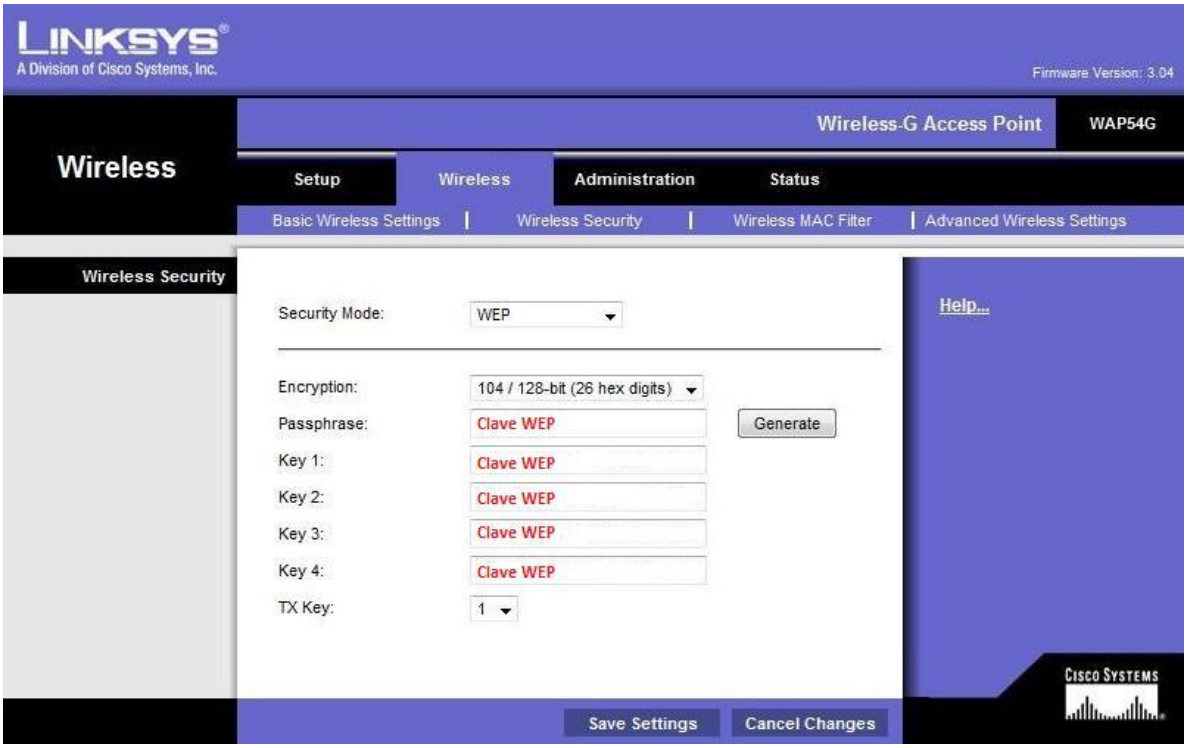


Figura 5-7 Uso de encriptación WEP

Uso de una VPN (Virtual Private Network)

Configurar una red privada virtual entre el origen y el destino. Utilizando una VPN se proporciona un túnel seguro independientemente del camino por el que circule la información, incluido Internet. Ya existen APs en el mercado que lo soportan.

Uso del estándar 802.1x

Nuevo estándar con el que permitimos autenticar al usuario entrante a nuestra WLAN. El servidor de autenticación no tiene que ser una máquina inteligente, por lo que pequeños APs podrán utilizar este estándar 802.1x. Es conocido como "Portal Cautivo", como el NoCat en Linux o los RADIUS y los TACACS+LDAP.

Utilizar el nuevo WPA (Wi-Fi Protected Access)

Mucho más fiable que el WEP siempre que no se utilicen claves inferiores a 20 caracteres y que no estén contenidos en un diccionario, ya que es susceptible de ataques. Este no es un problema puntual, es una indicación de la debilidad de WPA. Solamente debemos recordar de la necesidad de utilizar claves largas y que incluyan caracteres especiales.

En la nueva protección WPA la cadena ASCII que se introduce sirve de semilla para una clave en constante rotación, de forma que cada paquete de información lleva una clave completamente diferente a los anteriores.

La autenticación se basa en el estándar 802.1x que define un protocolo de autenticación por puerto, considerando cada frecuencia de radio como un puerto en el caso de las WLAN.

Uso de Firewall

Algunos AP traen incorporado un firewall para cerrar determinados puertos que impidan posibles ataques a nuestra WLAN, si el AP no dispone de un firewall integrado debemos configurar uno.

Como resumen, la mejor solución es utilizar varios de los puntos anteriores para poner trabas a los usuarios que no tienen autorización, si bien, impedir el acceso por completo es difícil.

5.5. Componentes instalados en la Red inalámbrica del IFUNAM

5.5.1. Punto de acceso Marca LinkSys modelo WAP54g

Los puntos de acceso (AP´s) son de la marca Link-Sys y el modelo es WAP54G, estos equipos tienen el respaldo de Cisco Systems, uno de los gigantes de la industria de las Telecomunicaciones a nivel mundial (Figura 5-8).

Figura 5-8 Punto de Acceso Inalámbrico LinkSys WAP54G

Las características de este punto de acceso son:

- Soporta los estándares 802.11b y 802.11g
- Las velocidades de conexión es de hasta 54Mbps
- Soportan seguridad WEP de 128 bits
- Tienen la capacidad de no anunciar (broadcast) el nombre de la red.
- Los usuarios pueden conectarse con sistemas operativos Windows, Linux, Windows CE, Palm y MacOS X.
- Pueden conectarse equipos que solo soportan el estándar 802.11b
- No cuentan con DHCP.

Configuración de los Puntos de Acceso Inalámbricos

Por las características de las instalaciones del Instituto de Física y para evitar el solapamiento de los canales en la WLAN, usaremos los canales que no se interfieren y se realizara la instalación de los equipos cuidando que no queden 2 puntos de acceso cercanos configurados con el mismo canal.

Las configuraciones de los equipos serán las siguientes:

- Nombre de la RED (SSID): NOMBRE
- Canal: 1, 6 u 11 (canales no solapados - evitar duplicidad en puntos de acceso cercanos)
- WEP Key: Clave de encriptamiento.
- Dirección IP estática: 192.168.2.x.
- Puerta de acceso (gateway): 192.168.2.x.
- Modo del punto de acceso: Punto de acceso, puente o repetidor.
- Propagación de SSID: deshabilitada.
- Modo de operación: Mixta, solo estándar G o solo estándar B.
- Nombre del dispositivo: Este nombre se compone de Edificio, piso y número, para ubicar si instalación física.

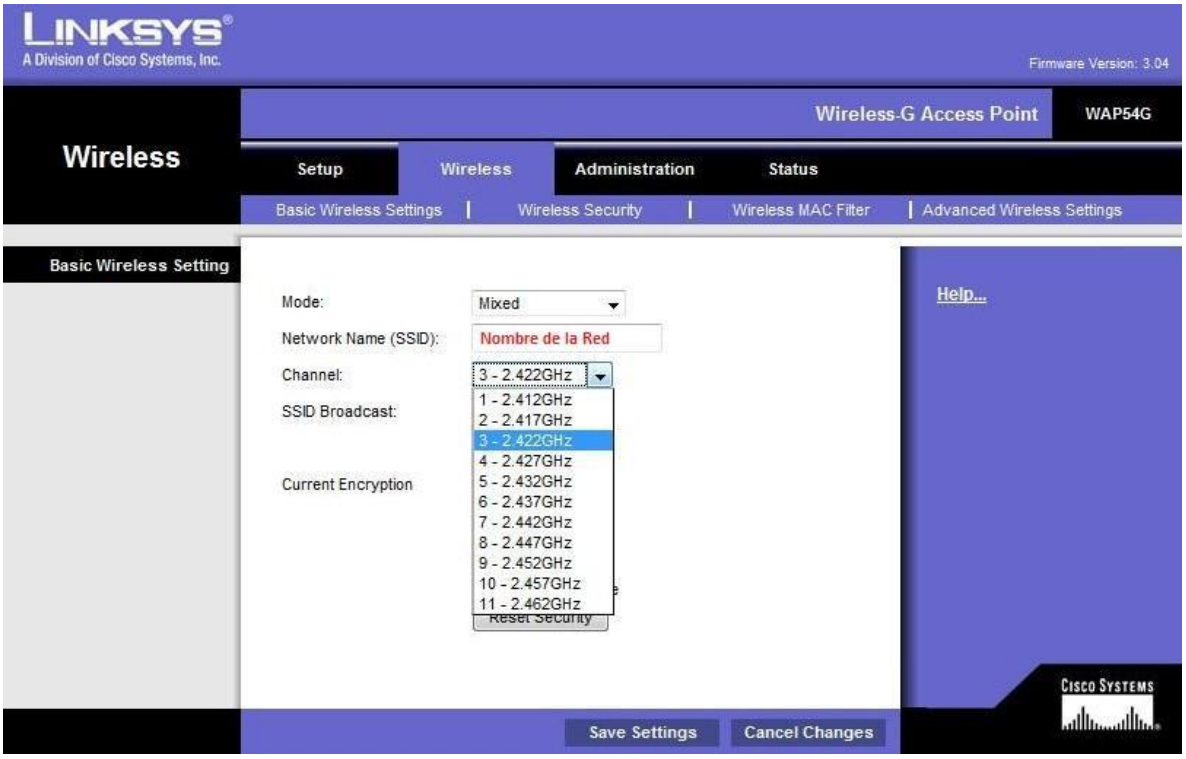


Figura 5-9 Configuración del Canal en un Punto de Acceso LinkSys

5.5.2. Servidor DHCP, NAT y Firewall

Debido a que los puntos de acceso instalados no traen el protocolo DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host), NAT (Network Address Translation – Traducción de Direcciones de Red) y Firewall incorporado se tuvo que instalar una computadora con Sistema Operativo OpenBSD en donde se configuro como servidor para estos protocolos y servicios.

Servidor DHCP

El protocolo DHCP permite a las computadoras o dispositivos de una red IP obtener sus parámetros (mascara de red, puerta de enlace y otros) de configuración automáticamente y también incluye un mecanismo de asignación de direcciones IP.

Sin DHCP, la dirección IP debe configurarse de forma manual en cada computadora o dispositivo, y si estas cambian de ubicación física a otro lugar de la red, hay que introducir una nueva dirección IP. DHCP permite al administrador de la red supervisar y distribuir las direcciones IP de forma centralizada enviando automáticamente una nueva dirección IP cada vez que una computadora se conecta en un lugar diferente de la red. DHCP usa el concepto de "alquiler" o "préstamo" de dirección IP, cuyo significado es que una dirección IP determinada será válida para una computadora durante un cierto período de tiempo. La duración del préstamo puede variar dependiendo de cuánto tiempo se le asigne en la configuración. DHCP es especialmente útil en el sector de educación y en otros entornos en los que los usuarios cambian con frecuencia.

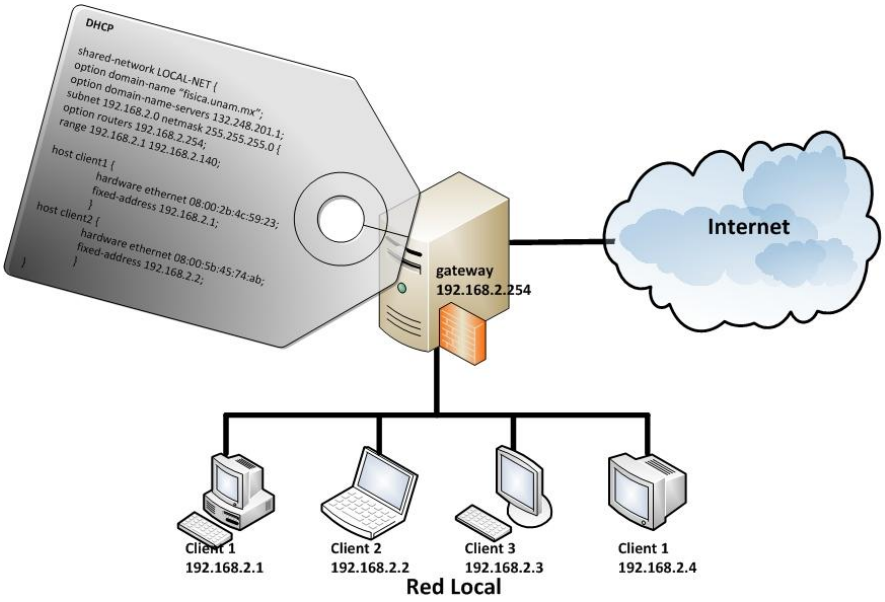


Figura 5-10 Diagrama de conexión de un servidor DHCP

Servidor NAT

Es una técnica que ha surgido en respuesta a la escasez de direcciones IPv4. Permite que una única dirección IP proporcione conectividad a un gran número de hosts. NAT en una red consiste en que todos los equipos usan uno de los rangos de direcciones privadas (estos rangos de direcciones no son enrutables). Para dirigir el tráfico a una puerta de enlace o proxy se necesita una dirección IP privada en el interior de la red y una IP homologada en el exterior a Internet.

RANGO		Tamaño de la red
Inicio	Fin	
10.0.0.0	10.255.255.255.255	/8
172.16.0.0	172.31.255.255	/12
192.168.0.0	192.168.255.255	/16

Rangos de direcciones privadas

Un enrutador NAT cambia la dirección origen en cada paquete de salida y dependiendo del método, también el puerto de origen para que sea único. Estas traducciones de direcciones se almacenan en una tabla para recordar que dirección y puerto le corresponde a cada dispositivo cliente y así saber a dónde deben regresar los paquetes de respuesta.

Si un paquete intenta ingresar a la red interna y no existe en la tabla de traducciones, el paquete es descartado. También se puede definir en la tabla de traducciones que un determinado puerto y dirección se pueda acceder a un determinado dispositivo, en este caso se le llama NAT inverso. (Figura 5-11)

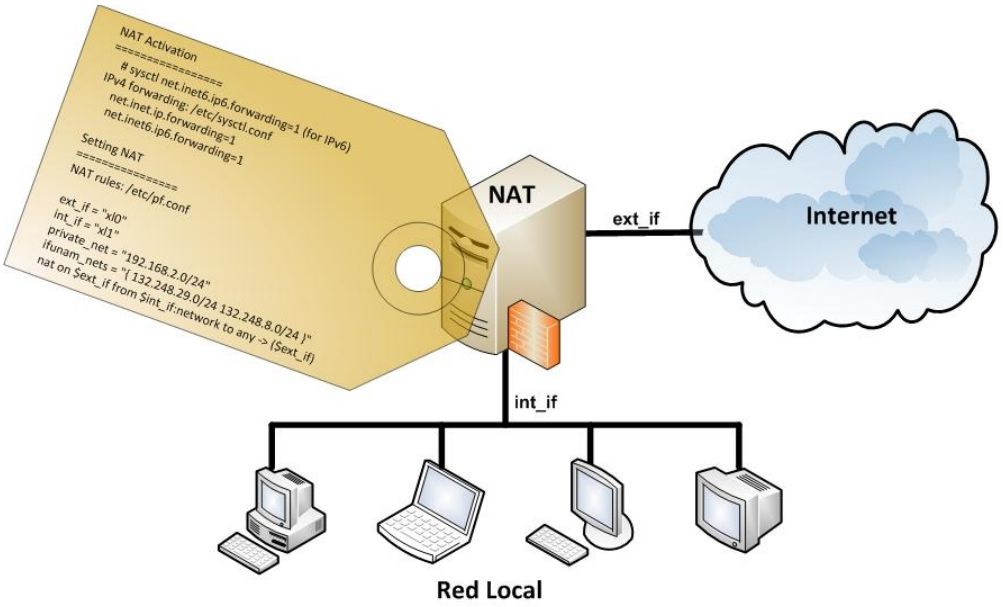


Figura 5-11 Diagrama de conexión de un servidor NAT

Firewall

Un firewall es un dispositivo que funciona como cortafuegos entre redes, es decir, sirve como filtro que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sea permite o deniega su paso. Para permitir o negar una comunicación el firewall examina el tipo de servicio al que corresponde y dependiendo de este, decide si lo permite o no. Además, el firewall examina si la comunicación es de entrada o salida y dependiendo de su dirección puede permitirla o no.

Un firewall puede bloquear aplicaciones que son innecesarias para nuestro trabajo. Dependiendo del tipo de firewall podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos negar o permitir algunos servicios como el de la WEB.

Un firewall puede ser un dispositivo de software o hardware y se conecta entre la red y el cable de la conexión a Internet.(Figura 5-12)

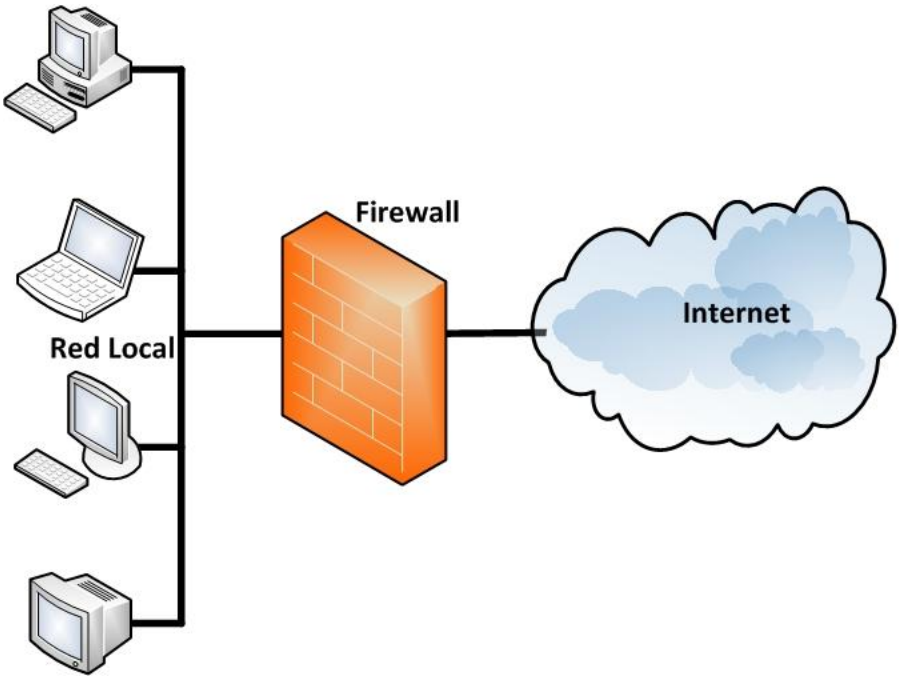


Figura 5-12 Diagrama de conexión de un firewall en una red

5.5.3. Configuración de la VLAN

Para contar con la administración centralizada de todos los puntos de acceso inalámbricos que se instalaron en el IFUNAM, se configuro una VLAN (Virtual LAN, "red de área local virtual") en los switches de la Red del Instituto de Física.

Una VLAN es un método de crear redes lógicamente independientes dentro de una misma red. Se pueden configurar varias VLANs en un mismo Switch o en una Red física. Las VLAN se emplean para reducir el tamaño del dominio de difusión (broadcast) y para la administración de la red separando segmentos lógicos de una red de área local que no deben intercambiar datos a través de la red, aunque pueden hacerlo a través de un enrutador o un switch capa 3. (Véase Figura 5-13)

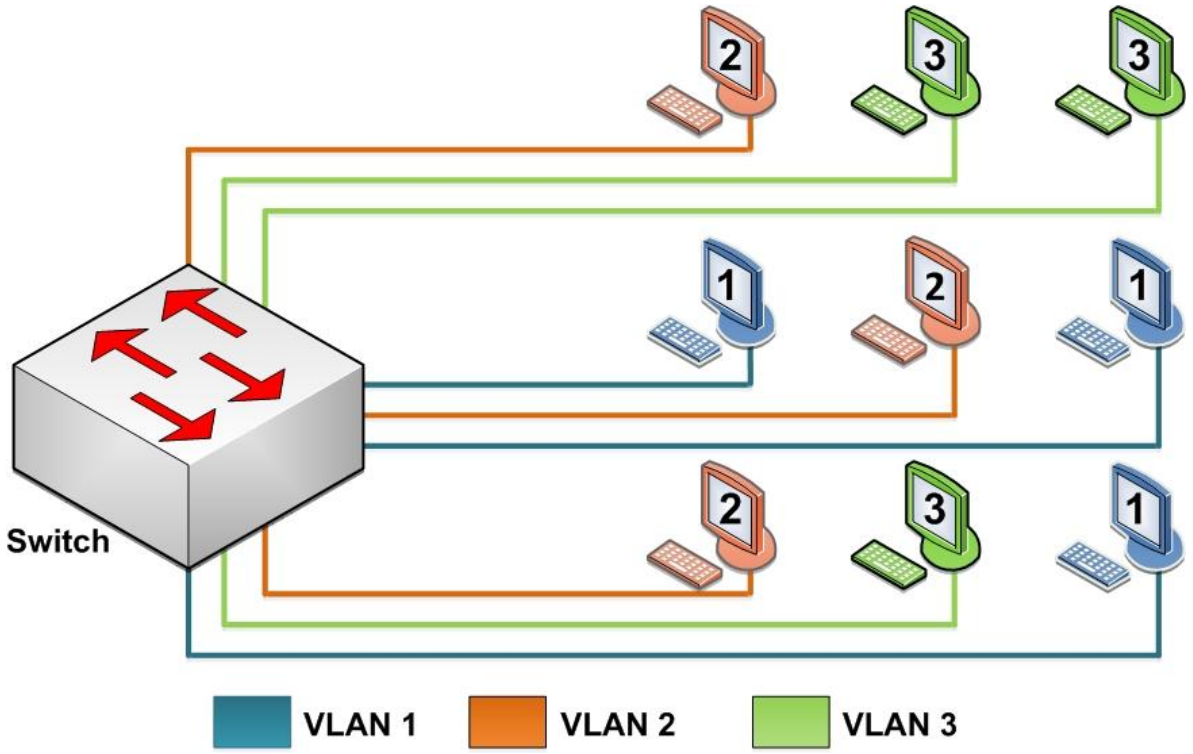


Figura 5-13 Configuración de una VLAN

Los puntos de acceso inalámbrico o computadoras conectados a una VLAN se comportan como si estuvieran conectados al mismo Switch, aunque la realidad es que están conectados físicamente en diferentes segmentos de una red de área local o en diferentes switches de la red.

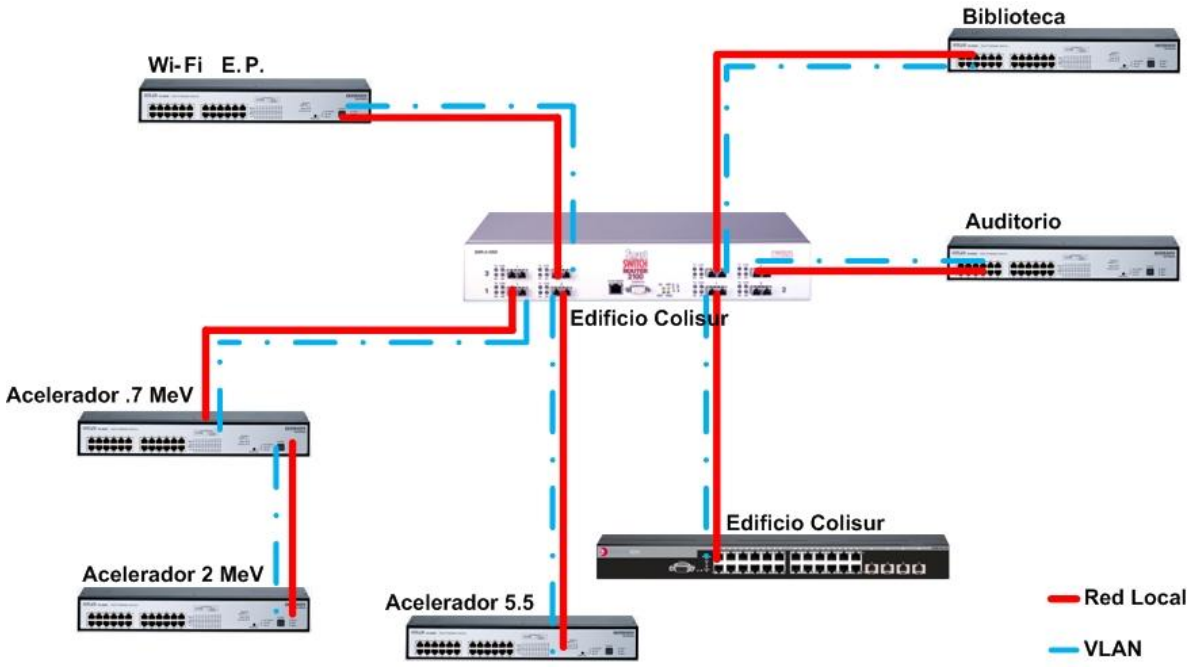


Figura 5-14 Diagrama de la VLAN para la red inalámbrica del IFUNAM

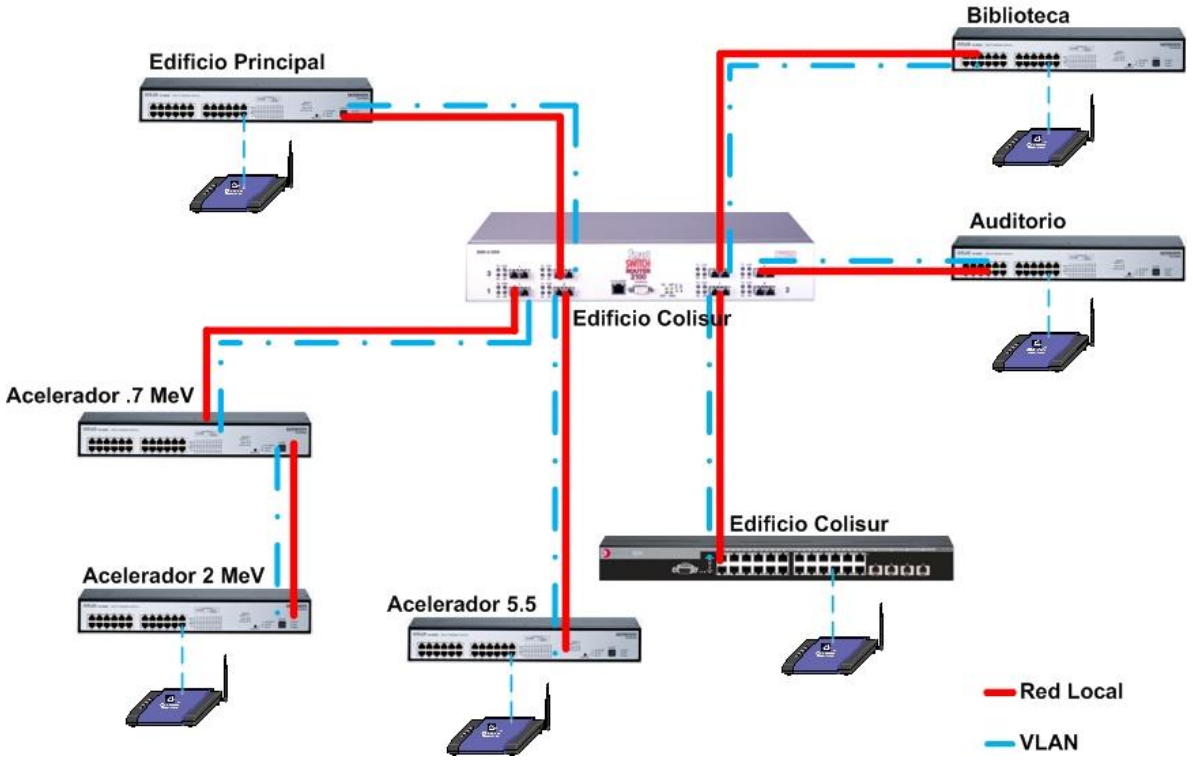


Figura 5-15 Diagrama de conexión de los puntos de acceso inalámbricos

Características de los equipos que conforman la Red del Instituto de Física.

Vertical Horizon VH-2402S 10/100/1000 Stackable Workgroup Switch

Características:

- 24 puertos 10/100 Mbps, 2 slots para expansión y un puerto serial para la administración.
- 1 puerto 1000Base-SX (MMF, conector tipo SC).
- Soporta streaming de aplicaciones de voz y video.
- Permite hasta 12,000 direcciones MAC.
- Soporta VLANs basadas en el estándar IEEE 802.1Q y se integra perfectamente en redes heterogéneas.
- Se puede apilar hasta 4 switches de 24 puertos mediante un modulo y cable STACK.
- Capacidad de rendimiento de 6.55 Mpps.
- Capacidad de ancho de banda de conmutación de 8.8 Gbps.

Vertical Horizon VH-8G Gigabit Ethernet standalone Workgroup Switch

Características:

- 8 puertos 1000Base-SX (MMF, conector tipo SC)
- Soporta streaming de aplicaciones de voz y video.
- Permite hasta 8k de direcciones MAC
- Soporta VLANs basadas en el estándar IEEE 802.1Q y se integra perfectamente en redes heterogéneas.
- Capacidad de rendimiento de 12 millones de pps.
- Capacidad de ancho de banda de conmutación de 16 Gbps.

SmartSwitch Router 2100

Características:

- 8 puertos 1000Base-SX (MMF, conector tipo SC)
- Procesador SmartSwitch ASIC para ruteo personalizado.
- Buffer de memoria de 3 Mb por puerto.
- Tabla de ruteo de hasta 50,000 rutas.
- Tabla de direcciones capa 2 de hasta 240,000 ingresos.
- Tabla de direcciones capa 3/4 de hasta 256,000 ingresos.
- Rendimiento de 8.0 Gbps sin bloqueo de conmutación de fabrica.
- Rendimiento de 9.2 millones de pps de enrutamiento.

5.5.4. Ubicación de los Puntos de acceso instalados

La red inalámbrica está diseñada con roaming y los usuarios pueden conectarse en: edificio principal, Acelerador 5.5 MeV, Acelerador 2 MeV, edificio Colisur, biblioteca y auditorio del Instituto de Física. Esta característica nos provee la movilidad de los usuarios sin que estos tengan que reconfigurar su conexión.

A continuación se muestra la ubicación de los equipos instalados en los diferentes edificios del Instituto de Física.

Edificio Principal

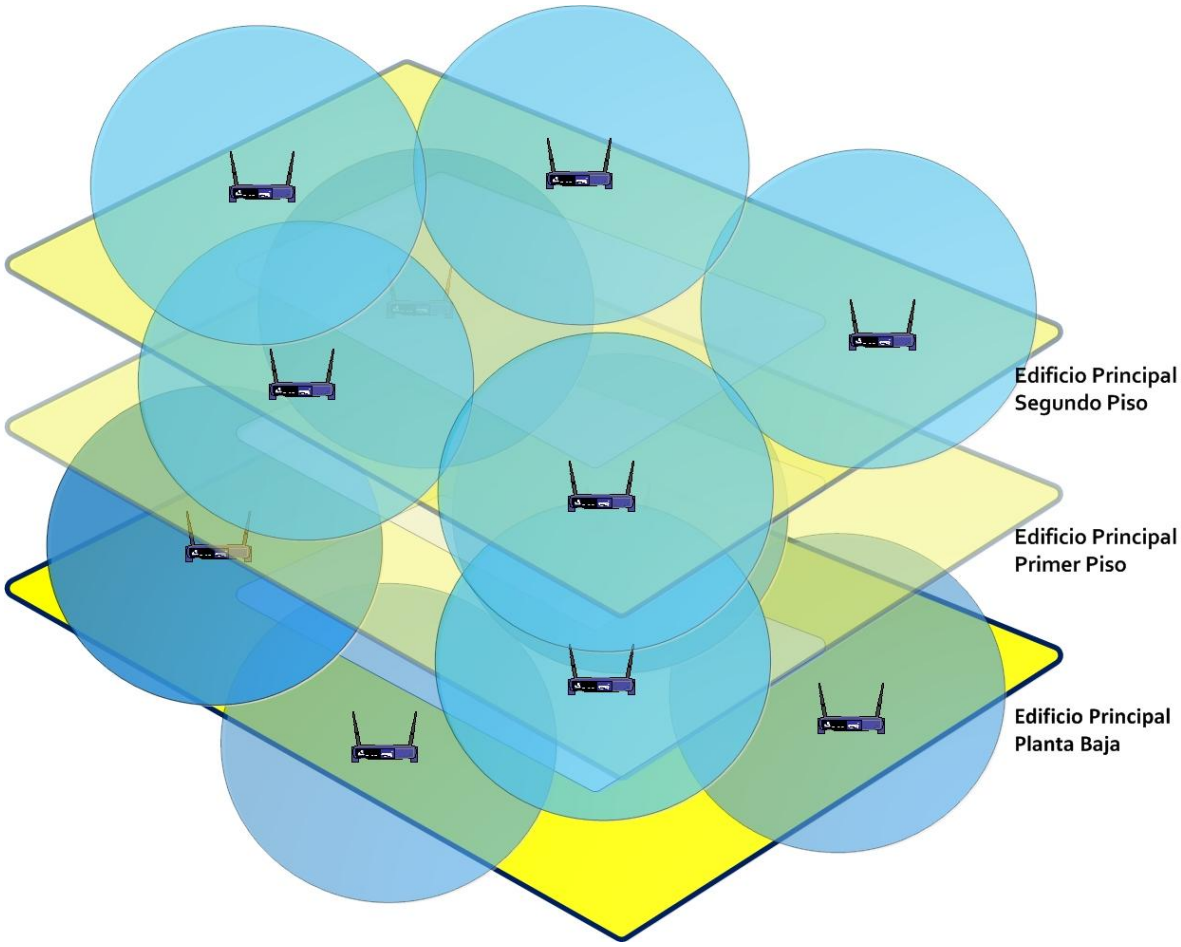


Figura 5-16 Ubicación de los puntos de acceso en el edificio principal

Edificio Colisur

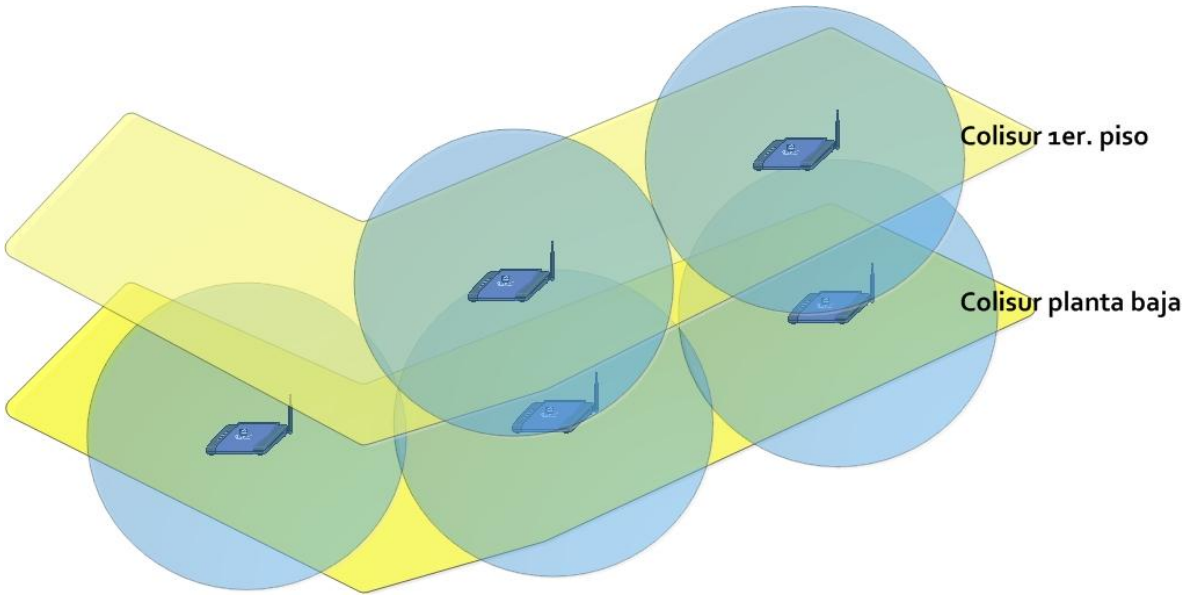


Figura 5-17 Ubicación de los puntos de acceso en el edificio Colisur

Biblioteca

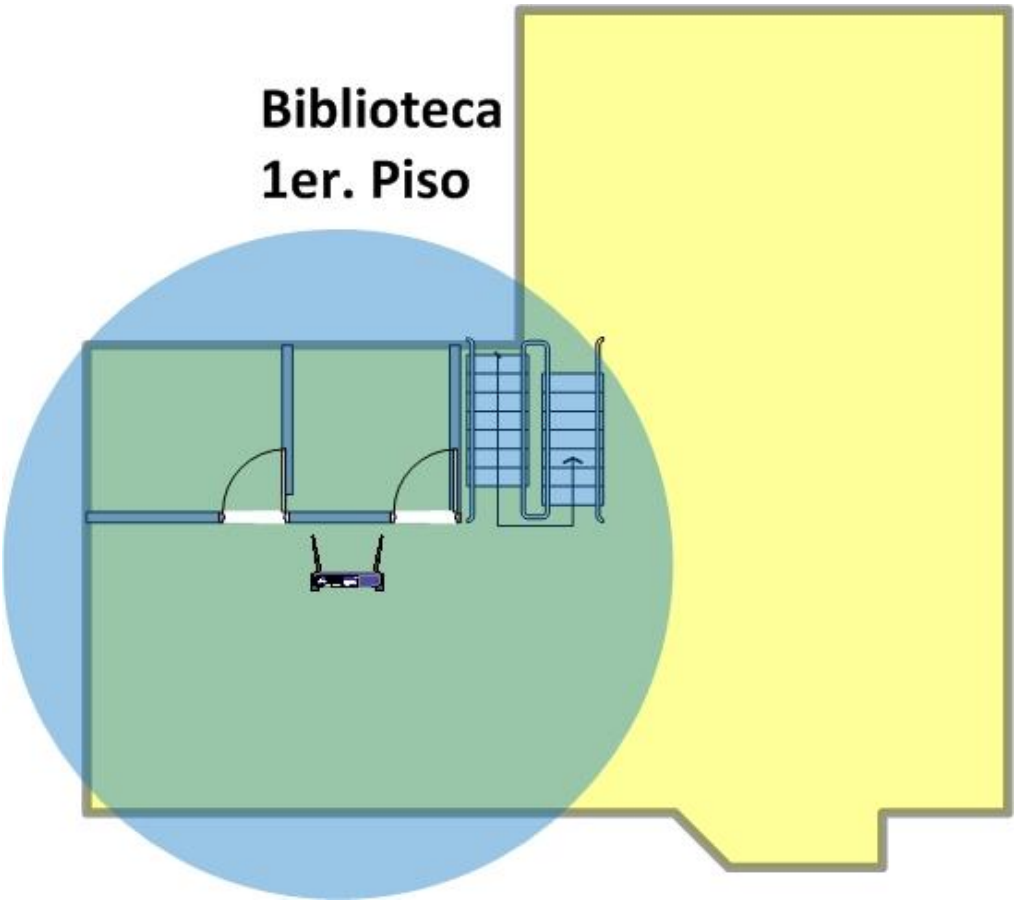


Figura 5-18 Ubicación de los puntos de acceso en la biblioteca

Auditorio

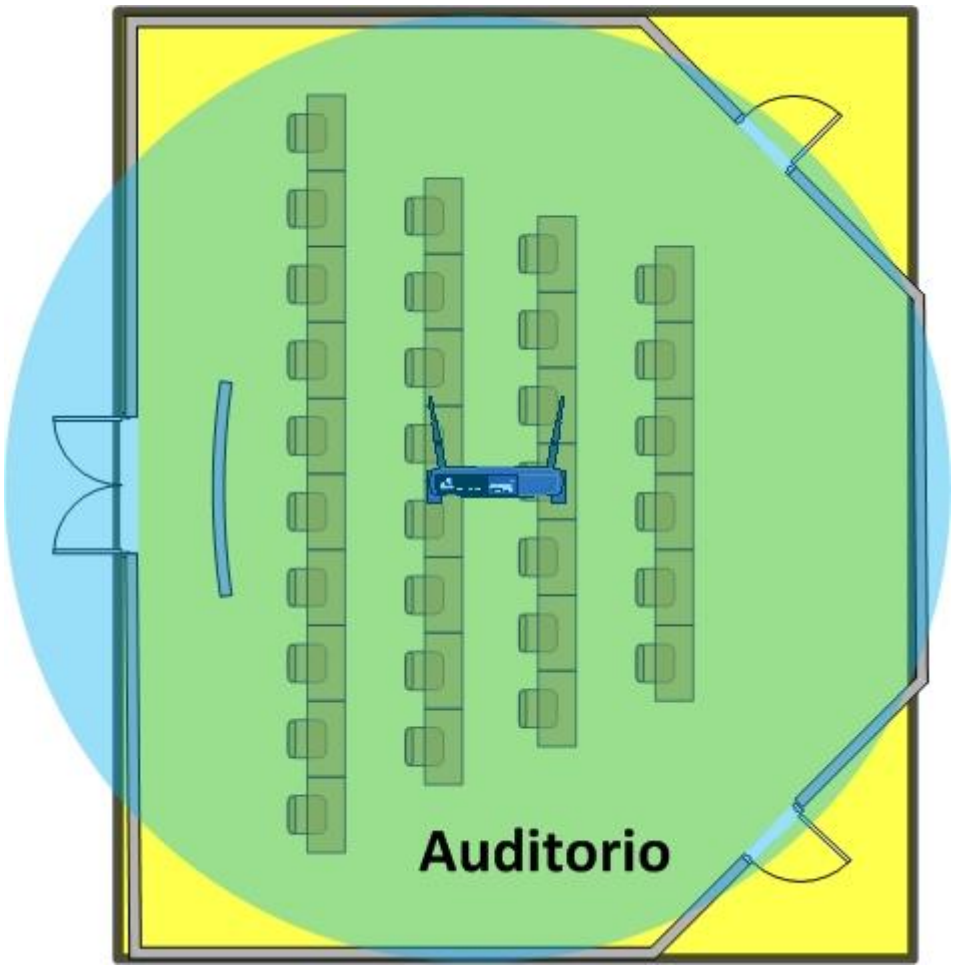


Figura 5-19 Ubicación de los puntos de acceso en el auditorio

Acelerador Van de Graff 2 MeV

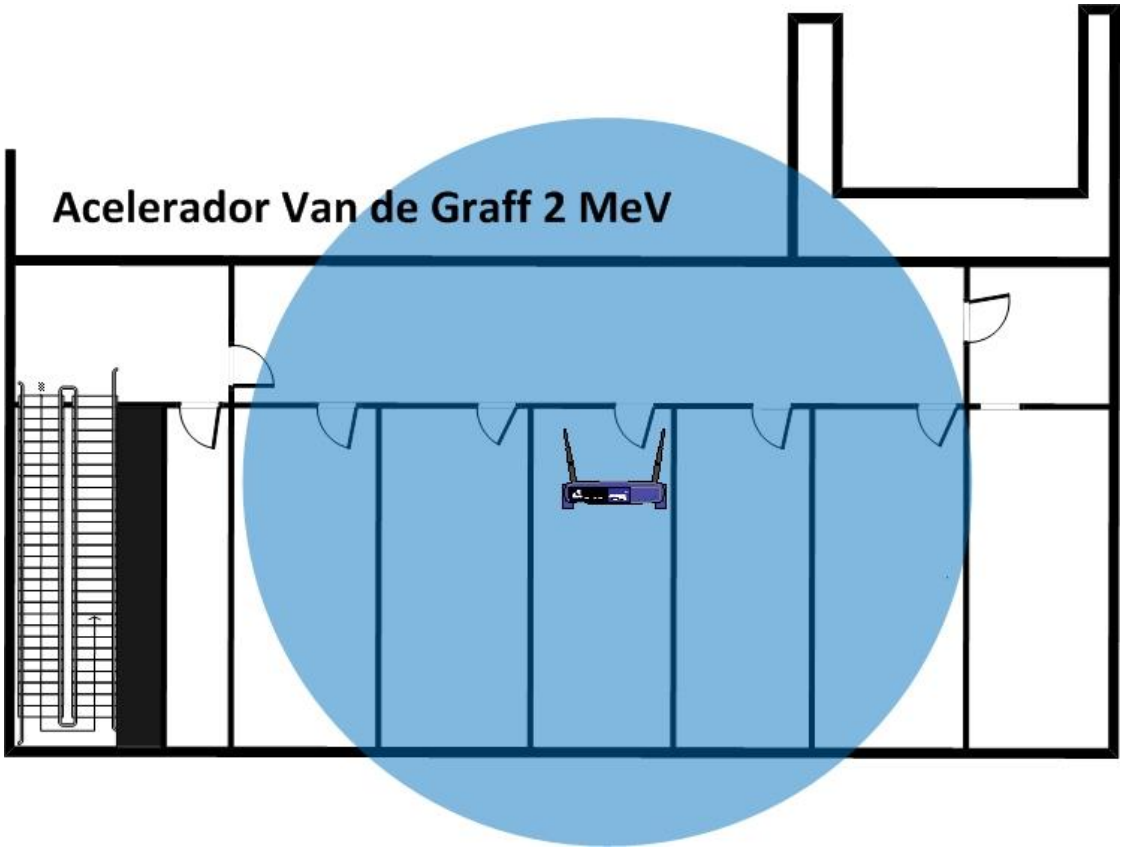


Figura 5-20 Ubicación de los puntos de acceso en el edificio Acelerador Van de Graff 2 MeV

Acelerador Van de Graff 5.5

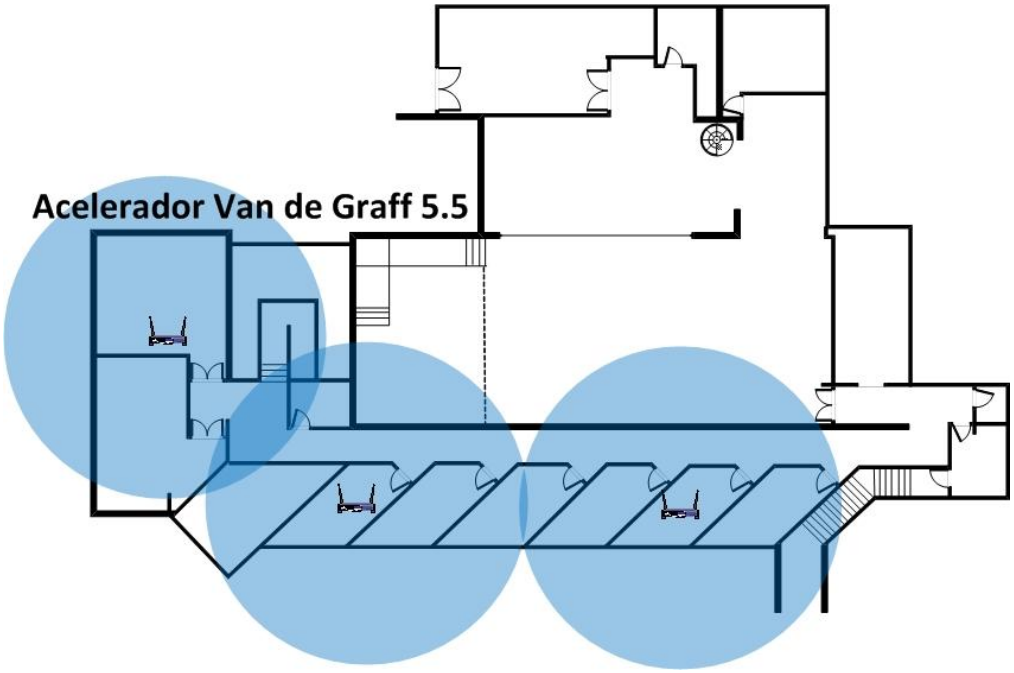


Figura 5-21 Ubicación de los puntos de acceso en el edificio Acelerador 5.5

Laboratorio de Microscopia Electrónica

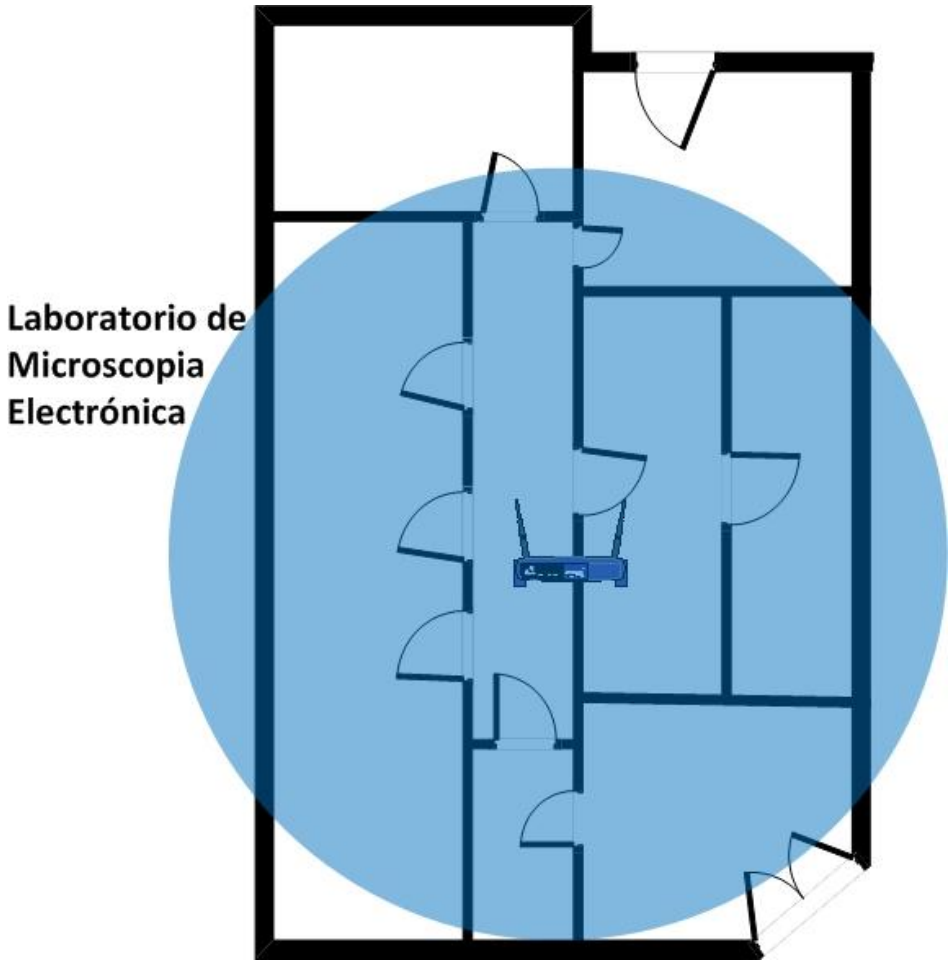


Figura 5-22 Ubicación de los puntos de acceso en el laboratorio de microscopia electrónica

Conclusiones

La limitada capacidad de nodos de la Red Ethernet y el creciente número de usuarios que ingresan diariamente al IFUNAM se convirtieron en un problema por la demanda de servicios de conectividad a la red e Internet. El plantear un proyecto para la instalación de más nodos de red resultaba poco costeable debido a la cantidad de puertos necesarios para cubrir dicha demanda de servicios.

Por esta causa, optamos por apostar a la tecnología sin cables, la cual es mas económica comparada con la inversión que requiere la alternativa con cables y por la falta de disponibilidad de espacios para instalar canaletas y nodos.

La inversión financiera del proyecto de la red inalámbrica fue relativamente económica, y ese era uno de los problemas a resolver de este trabajo de tesis, ya que se contó con un presupuesto limitado. Al tomar como punto de partida la infraestructura de nuestra red Ethernet, la parte de la conectividad para la administración y mantenimiento de los equipos de la red inalámbrica quedó resuelto gracias a la configuración de la red local virtual (VLAN). Además, los de Puntos de Acceso que utilizamos son de excelente calidad, sin ser equipos profesionales cubren perfectamente nuestras necesidades de cobertura geográfica de señal inalámbrica de datos y por lo cual el costo es razonablemente accesible para el presupuesto que la institución asignó a este proyecto.

Al implementar la solución inalámbrica fue posible hacer una redistribución de direcciones IP a los usuarios permanentes del Instituto de Física, así como a los cubículos y laboratorios que ya contaban con un nodo físico de red Ethernet. De este modo, los usuarios que no tiene asignado un cubículo o que solo están temporalmente se les puede facilitar el acceso a la red inalámbrica, tomando en cuenta que cada vez es más común que los usuarios cuenten con equipos de computo portátiles con características de conexión Wi-Fi.

El simple hecho de no depender de un cable para tener acceso a la red del Instituto de Física es una de las ventajas principales de este proyecto, ya que facilita la movilidad de los usuarios en caso de ser necesario. Como usuario de este servicio, he de mencionar lo práctico que es mantenerse en línea dentro de las instalaciones no importando el cambio de ubicación ya sea un cubículo, laboratorio, auditorio o la biblioteca sin necesidad solicitar la conexión mediante el uso de un cable de red.

Los usuarios, por el tipo de actividades que desarrollan dentro del Instituto de Física, requieren mantener su comunicación y consulta de datos activa, por lo que el tener acceso a una red inalámbrica les facilita reubicarse fácilmente dentro de estas instalaciones.

Una vez realizada la instalación del a Red Local Inalámbrica del Instituto de Física de la UNAM, se logro comprobar la hipótesis planteada.

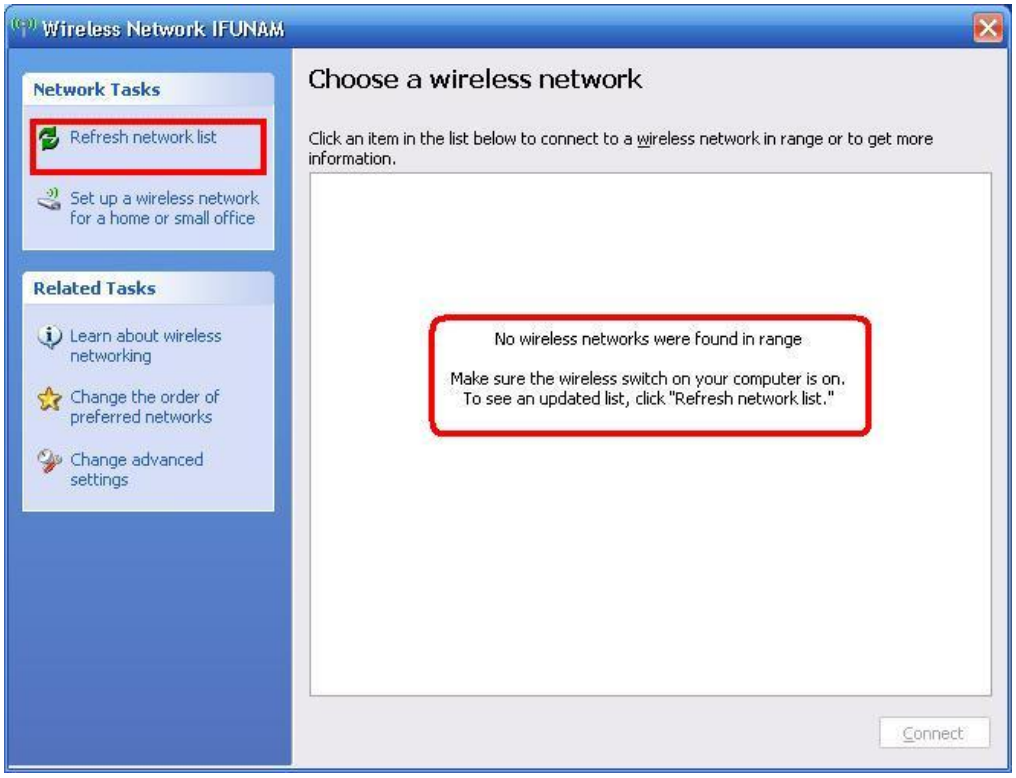
Apéndices

Apéndice A

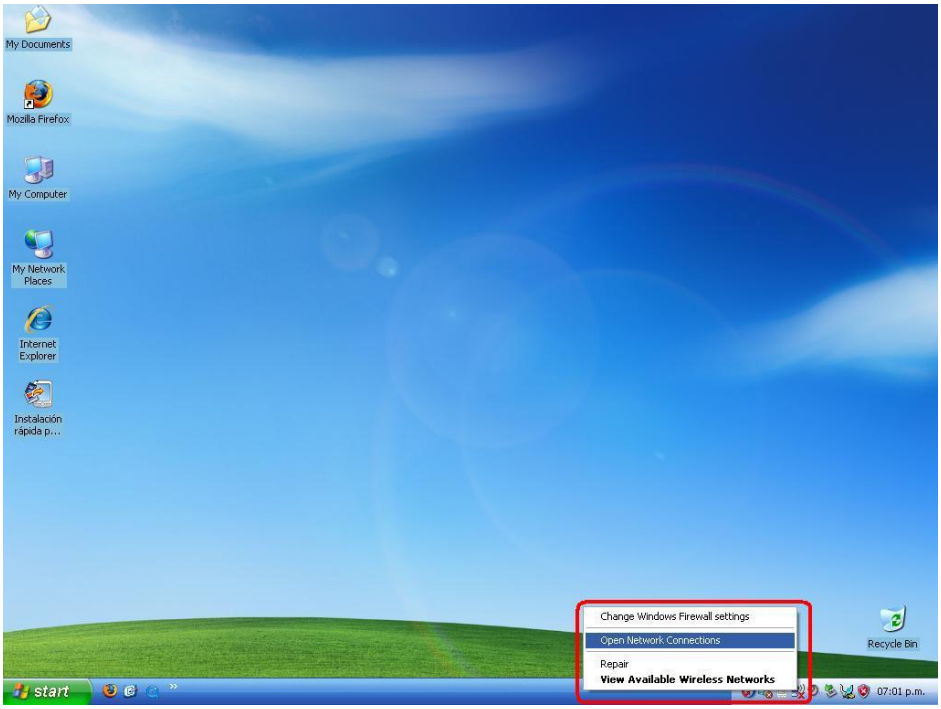
Configuración de la Red Inalámbrica con Windows XP

1. – Primero que todo, asegúrese que su Laptop tenga Adaptador de Redes Inalámbricas y que se encuentre activado.

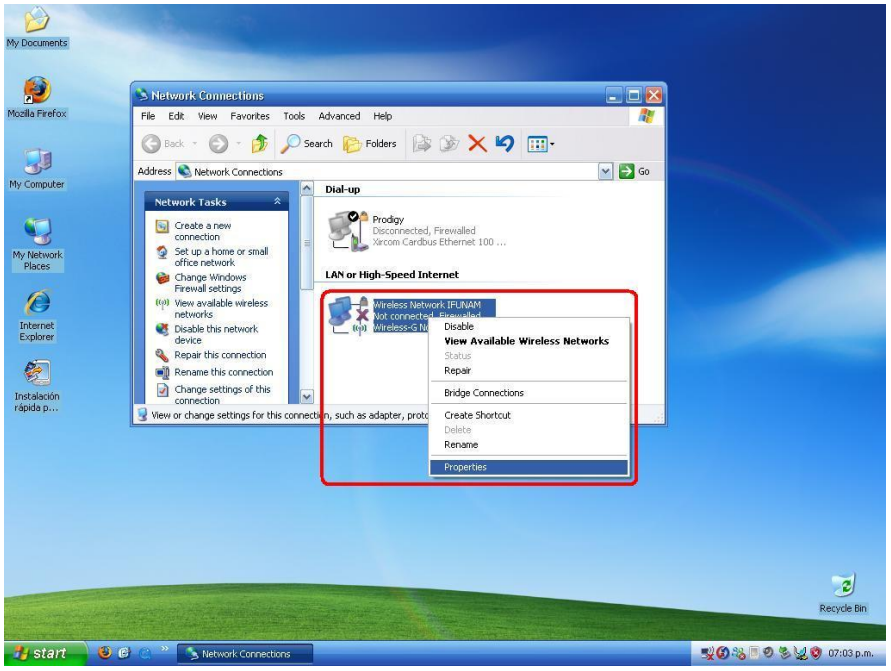
2. – Haga click en el icono de Conexión de red inalámbrica que se encuentra en la barra de tareas de Windows XP, en seguida aparecerá la ventana de Redes Inalámbricas Disponibles como se aprecia en la siguiente imagen. En la lista no aparece el nombre de la red inalámbrica del Instituto, recordemos que por seguridad hemos deshabilitado (*SSID broadcast DISABLE*) la difusión del nombre de la red, por lo que no se podrá visualizar en la ventana de **redes inalámbricas disponibles**



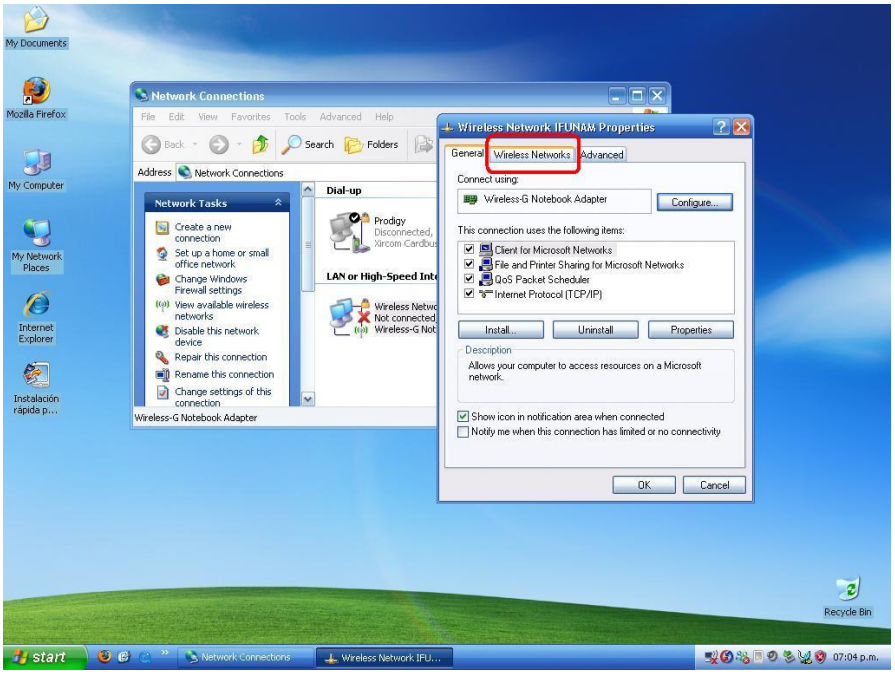
3. – Para configurar la conexión de la red inalámbrica hacemos click derecho en el icono de la conexión de **red inalámbrica** que se encuentra en la **barra de tareas de Windows XP**, como se muestra en la figura siguiente



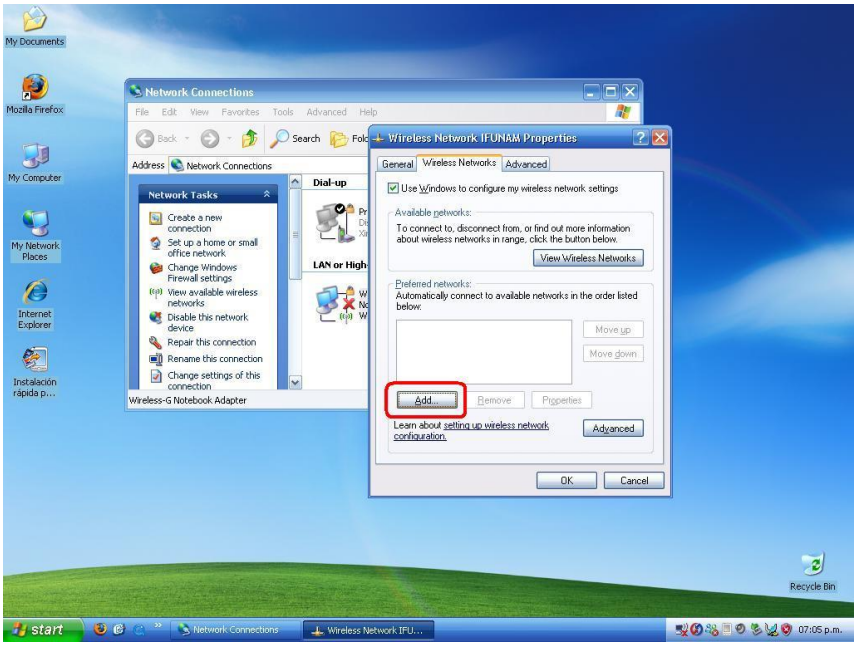
4. – En seguida nos abre la ventana de las **Conexiones de Red**, seleccionamos con el botón derecho del mouse la *Conexión de Red inalámbrica* y seleccionamos **Propiedades**, como se muestra en la figura siguiente



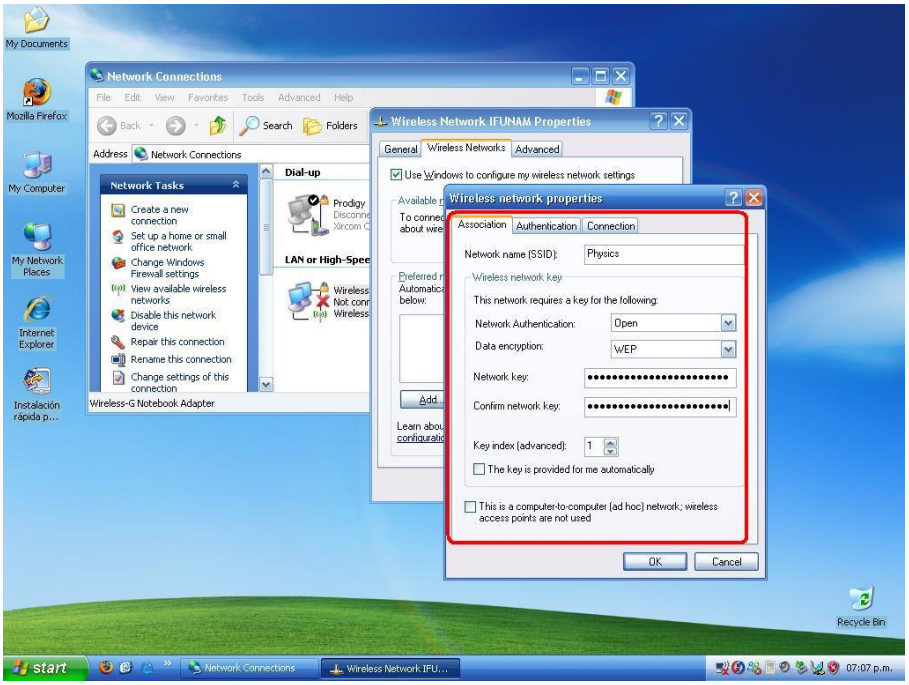
5. – En seguida nos abre la ventana de las propiedades de la conexión de ***Red Inalámbrica***, y seleccionamos **Redes Inalámbricas**, como se muestra en la figura siguiente



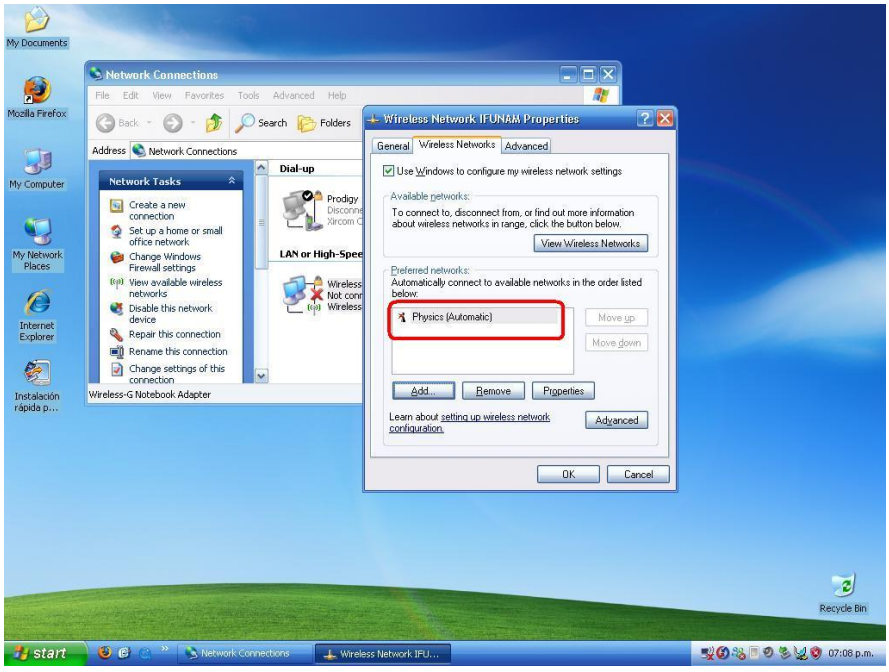
6. – En el cuadro de *Redes Preferidas* esta vacio, por lo que debemos agregar la configuración de nuestra red, damos click en el botón **Agregar**, como se muestra en la figura siguiente



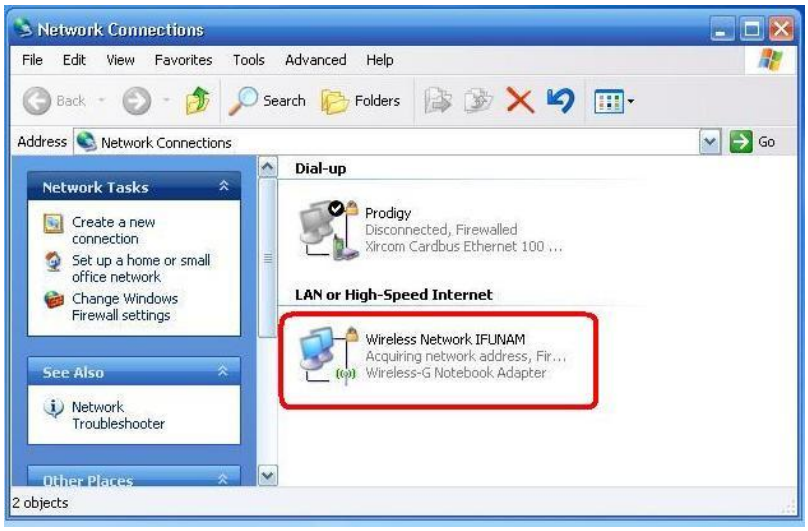
7. – En seguida nos abre la ventana para proporcionar los datos de la conexión, en esta debemos poner el **Nombre de la Red**, la autenticación que es Abierta, la **encriptación de datos** que usa y la **Clave de la Red** (WEP) y hacemos click en el botón **Aceptar**, como se muestra en la figura siguiente

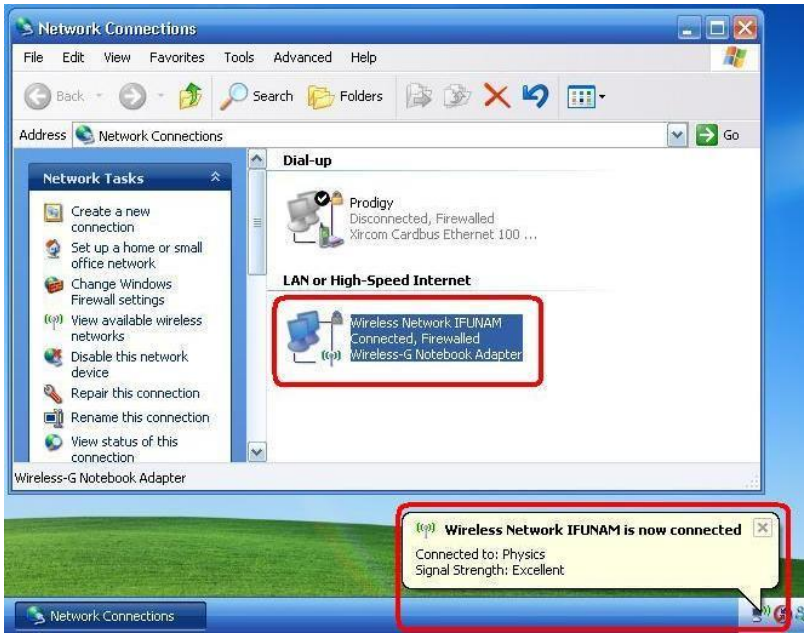


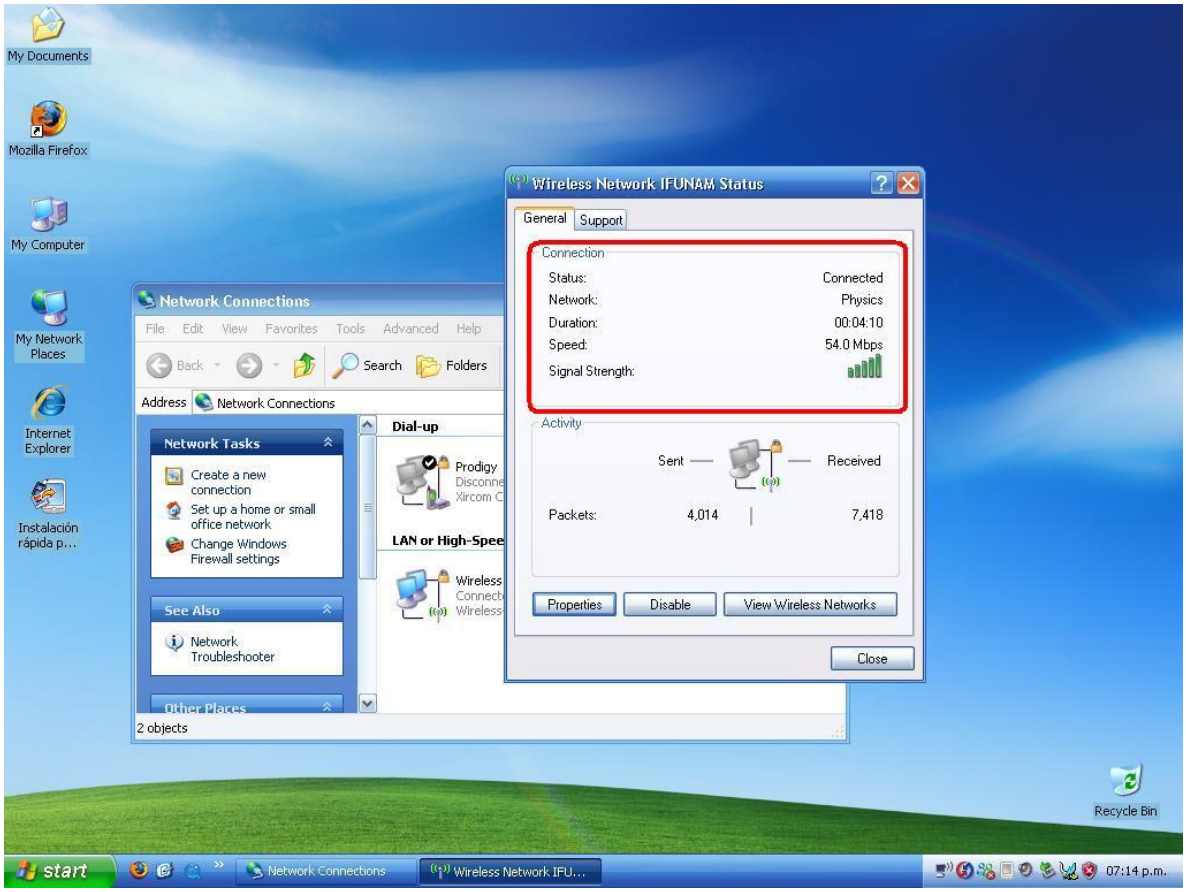
8. – En seguida nos muestra la red configurada en la ventana de **Redes preferidas** y hacemos click en el botón **Aceptar**, como se muestra en la figura siguiente



9. – En seguida nos muestra haciendo la **autoconfiguración de la dirección de la red** y finalmente nos muestra que estamos **conectados a la red**, como se muestra en las siguientes figuras





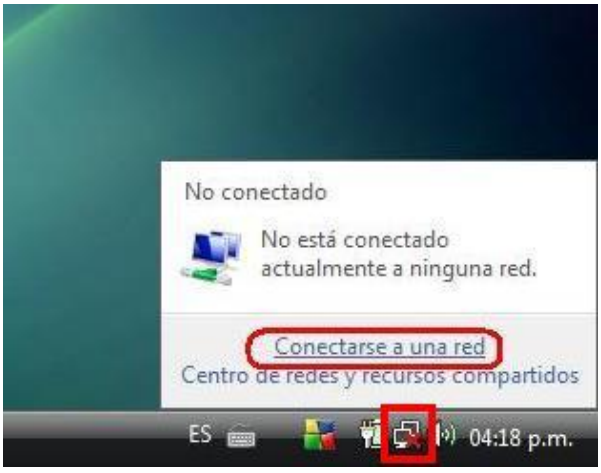

My Documents
Mozilla Firefox
My Computer
My Network Places
Internet Explorer
Instalación rápida p...
Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
See Also
Network Troubleshooter
Other Places
Dial-up
Prodigy
LAN or High-Spee
2 objects
Wireless Network IFUNAM Status
General Support
Connection
Status: Connected
Network: Physics
Duration: 00:04:10
Speed: 54.0 Mbps
Signal Strength:
Activity
Sent Received
Packets: 4,014 7,418
Properties Disable View Wireless Networks
Close
Recycle Bin
start
Network Connections
Wireless Network IFU...
07:14 p.m.

Apéndice B

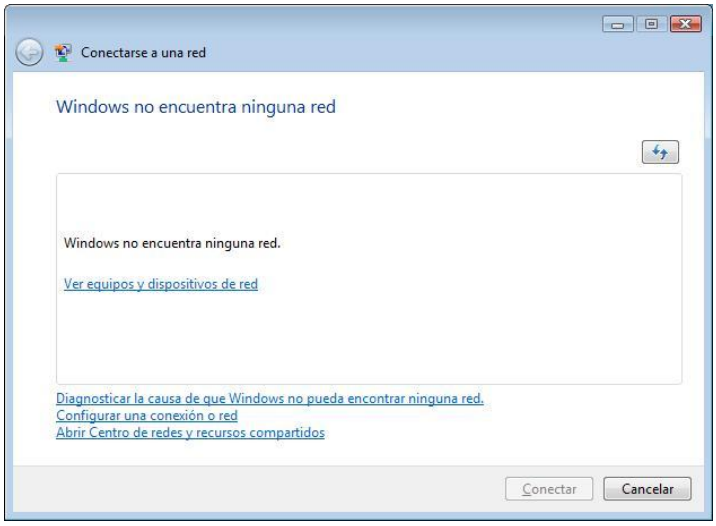
Configuración de la Red Inalámbrica con Windows Vista

1. – Primero que todo, asegúrese que su Laptop tenga Adaptador de Redes Inalámbricas y que se encuentre activado.

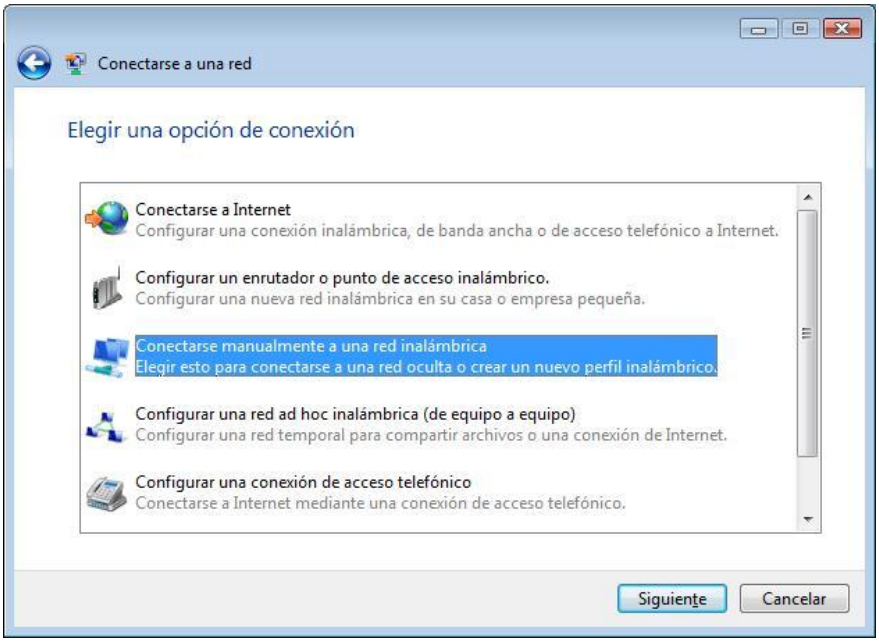
2. – Haga click en el icono de Conexión de red que se encuentra en la barra de tareas de Windows Vista, en seguida aparecerá una ventana emergente que nos indica que **no estamos conectados,** en esta ventana seleccionamos ***Conectarse a una red*** como se muestra en la figura siguiente:



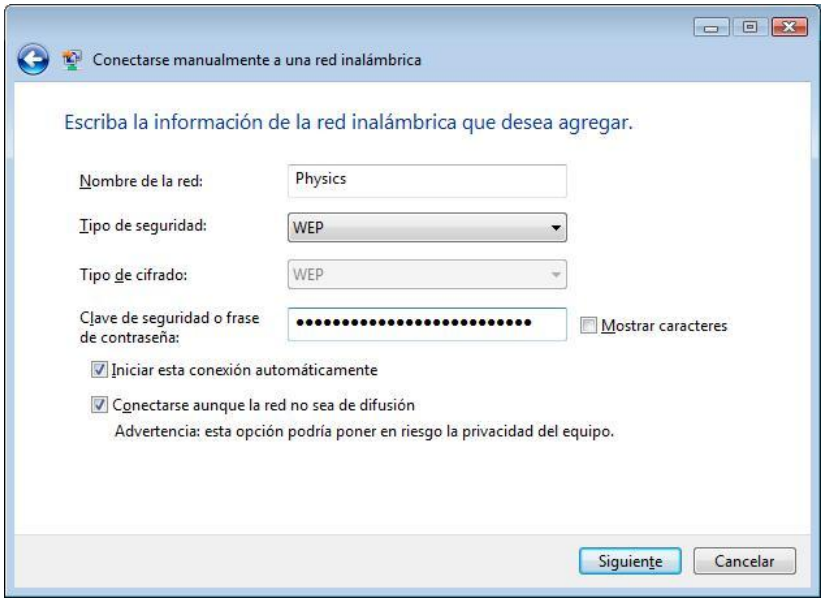
3. – En seguida aparecerá la ventana **Conectarse a una red** como se aprecia en la siguiente imagen y nos informa que Windows no encuentra ninguna red. Elegimos la opción Configurar una conexión o red haciendo doble click con el mouse.



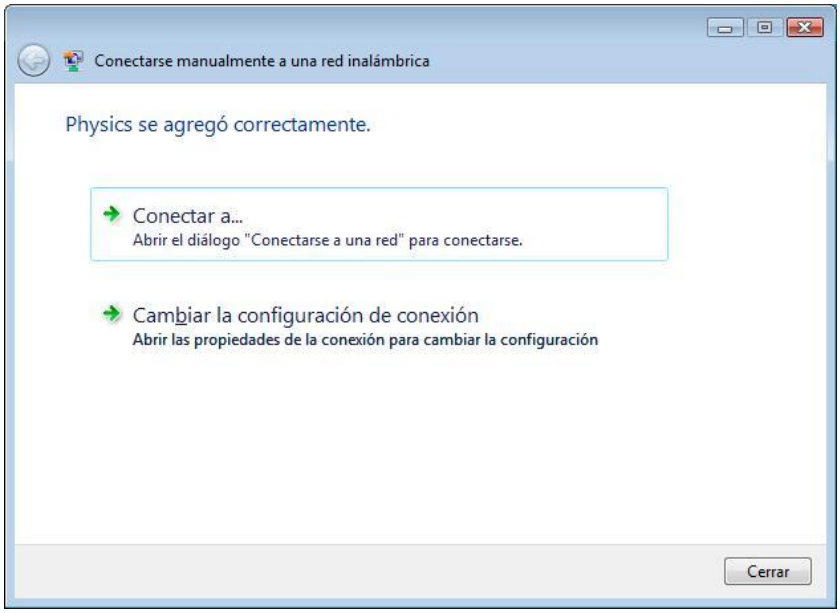
4. – En seguida aparecerá la ventana **Conectarse a una red** en esta seleccionamos la opción **Conectarse manualmente a una red inalámbrica**, y le damos siguiente, como se muestra en la figura.



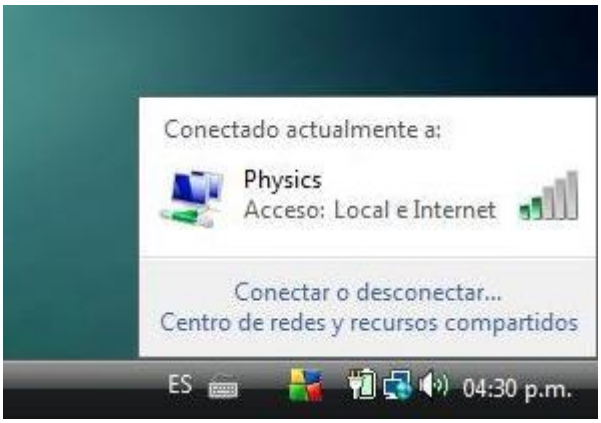
5. – En la ventana **Conectarse manualmente a una red inalámbrica** proporcionamos todos los datos de la configuración de la red inalámbrica del Instituto de Física. En esta ventana ponemos el nombre de la red (Physics), el tipo de seguridad WEP 128 bits, seleccionamos las opciones: *Iniciar esta conexión automáticamente* y *Conectarse aunque la red no sea de difusión*, y presionamos el botón siguiente, como lo indica la figura de abajo.

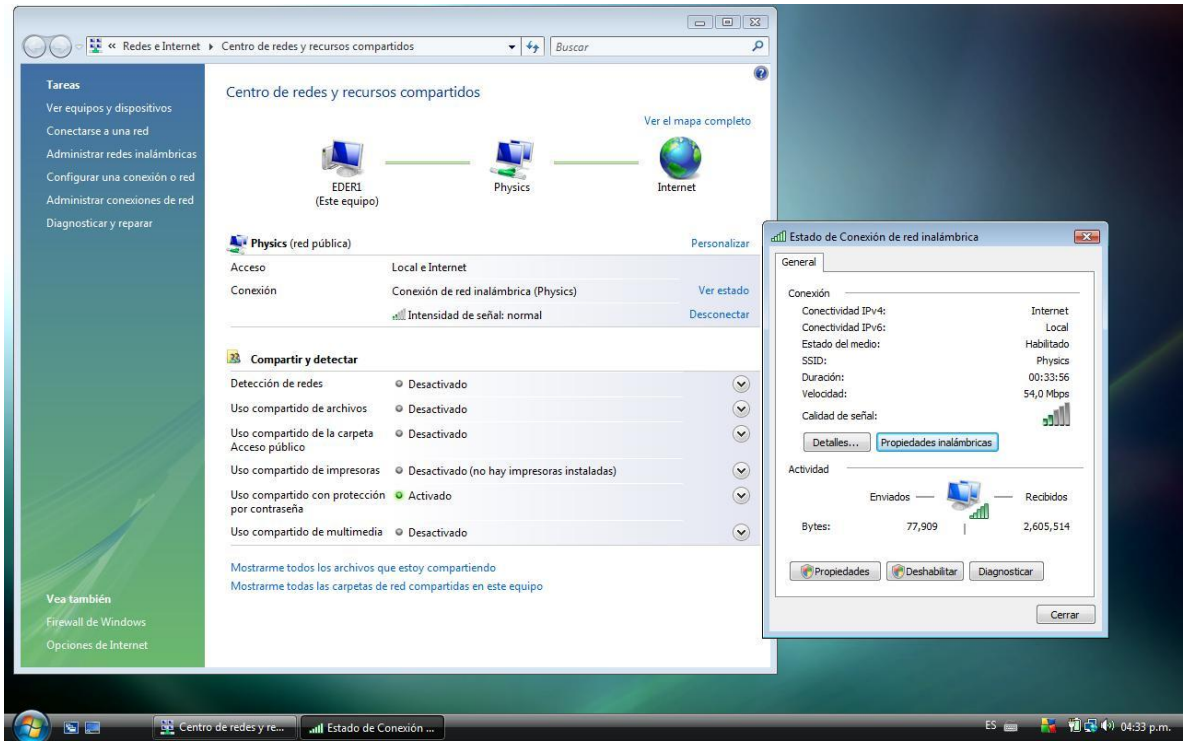


6. – En la ventana **Conectarse manualmente a una red inalámbrica** nos indica que la Red o conexión con nombre Physics se agregó correctamente y presionamos el botón cerrar.



7. – A continuación mediante un mensaje emergente en la barra de tareas nos indica que nos hemos conectado a la red o conexión inalámbrica **Physics**, como se lo indican las siguientes figuras.





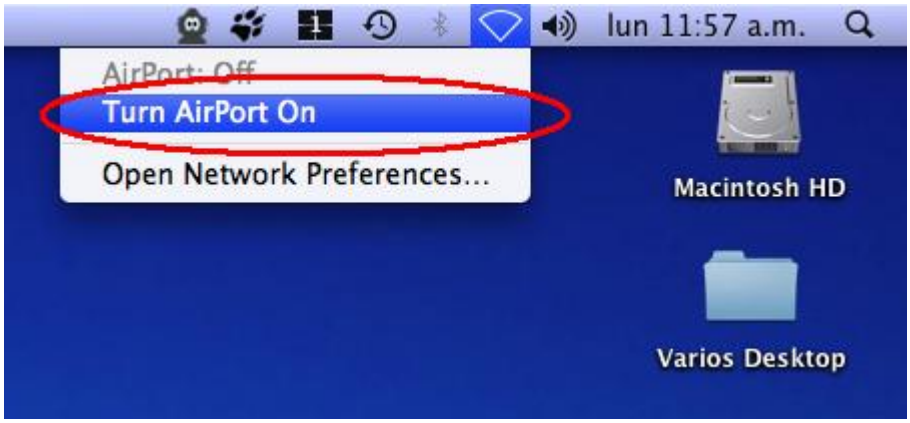
Apéndice C

Configuración de la Red Inalámbrica con Macintosh

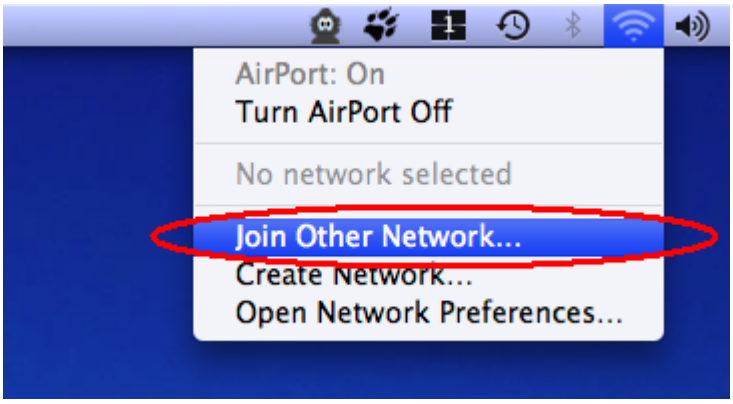
La red inalámbrica es compatible con dispositivos inalámbricos que operan bajo los estándares 802.11b y 802.11g.

Esta guía ayudará a configurar su equipo de cómputo personal, laptop o PDA la conexión a la Red inalámbrica del Instituto de Física de la UNAM.

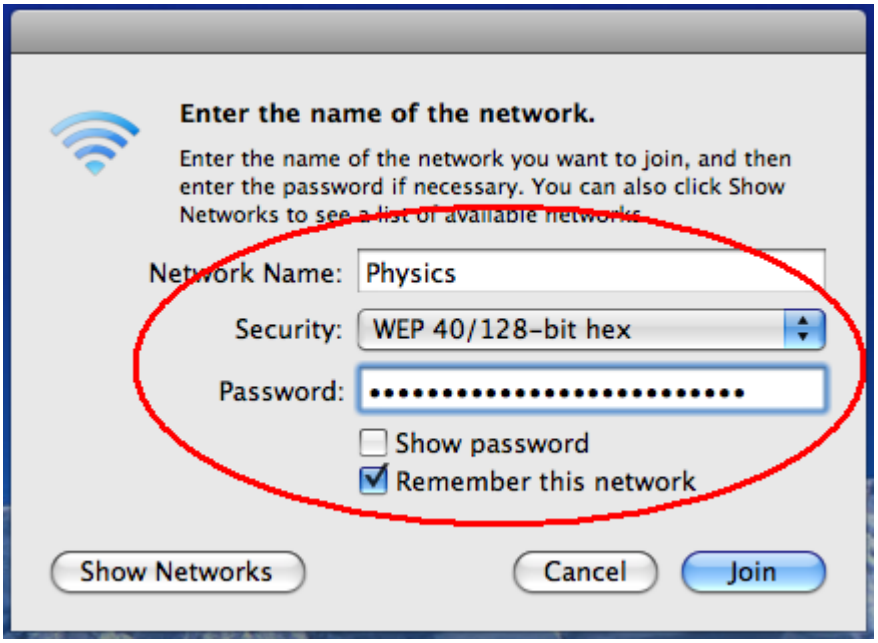
1. – Habilitar la tarjeta de red inalámbrica y dar click en **Turn AirPort On**, como se muestra en la sigte. Figura.



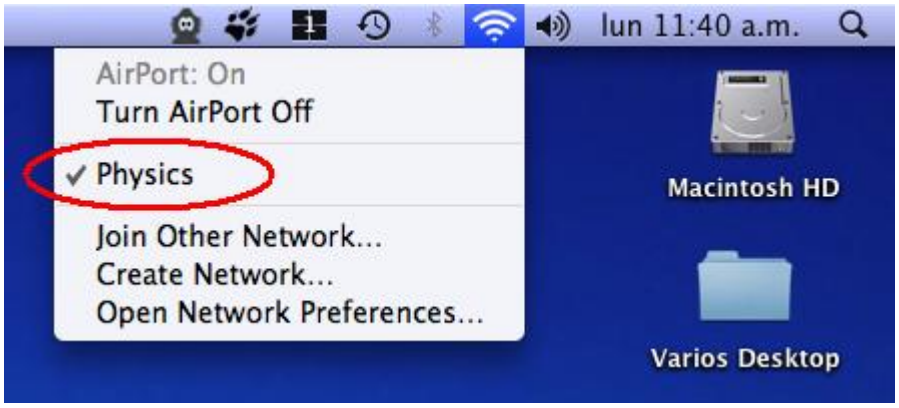
2. – Una vez que la tarjeta de red inalámbrica ya esta activa, damos click en **Joint Other Network…** para configurar los parámetros de la red inalámbrica del Instituto de Física, como se muestra en la siguiente figura.

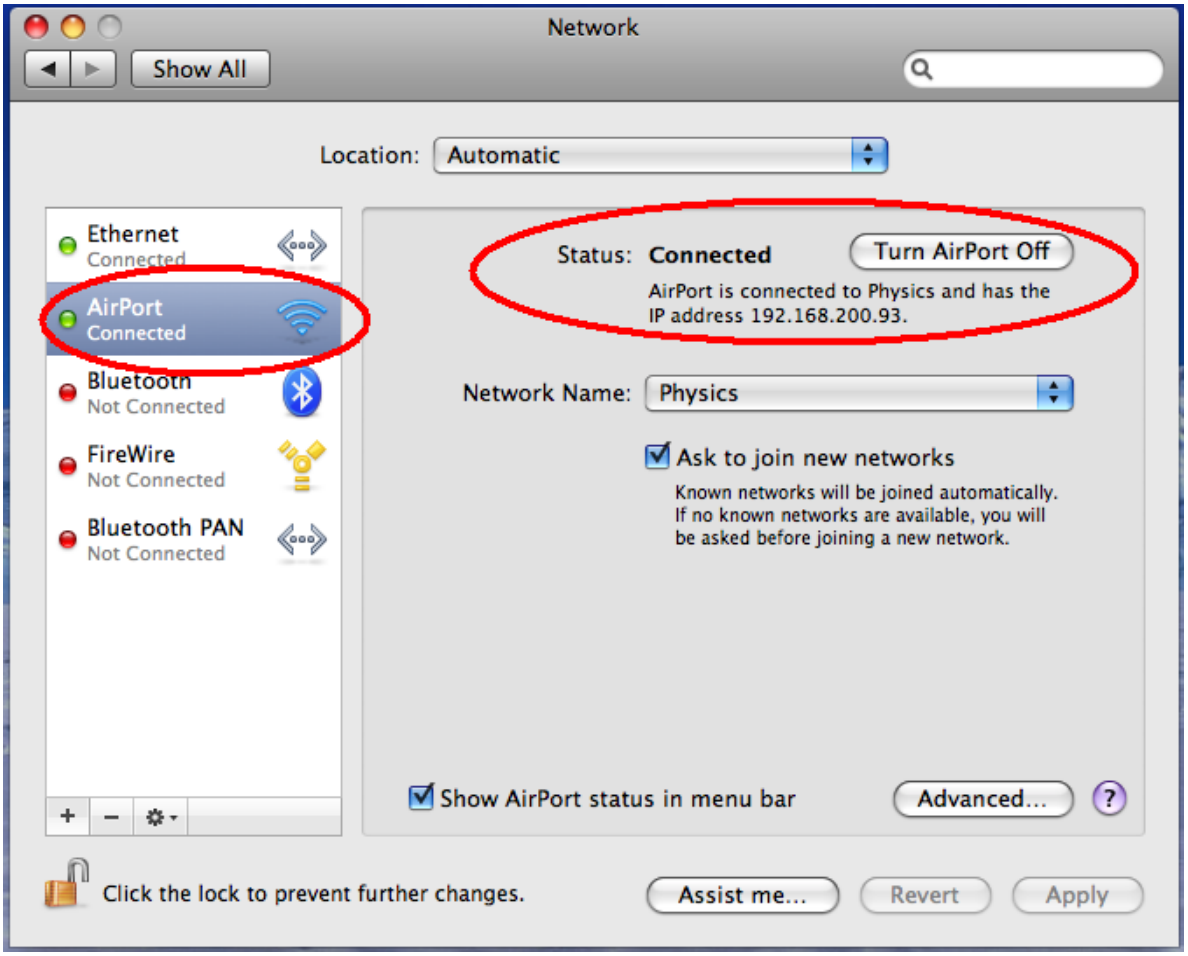


3. – Ingresamos el nombre de la red en el campo **Network Name** y en **Security** ingresamos la clave **WEP** de la Red inalámbrica del Instituto y seleccionamos **Remember this Network**, y damos click en Join. Tal como se muestra en la siguiente figura.



4. – En estos momentos ya debemos tener dado de alta la configuración de la red inalámbrica para el Instituto, solamente tendrá que verificar quela PC o dispositivo inalámbrico ya esté conectado a la Red. Como lo muestran las siguientes figuras.


lun 11:40 a.m.
AirPort: On
Turn AirPort Off
Physics
Join Other Network...
Create Network...
Open Network Preferences...
Macintosh HD
Varios Desktop


Network
Show All
Location: Automatic
Ethernet
Connected
AirPort
Connected
Bluetooth
Not Connected
FireWire
Not Connected
Bluetooth PAN
Not Connected
Status: Connected
Turn AirPort Off
AirPort is connected to Physics and has the IP address 192.168.200.93.
Network Name: Physics
Ask to join new networks
Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.
Show AirPort status in menu bar
Advanced...
Click the lock to prevent further changes.
Assist me...
Revert
Apply

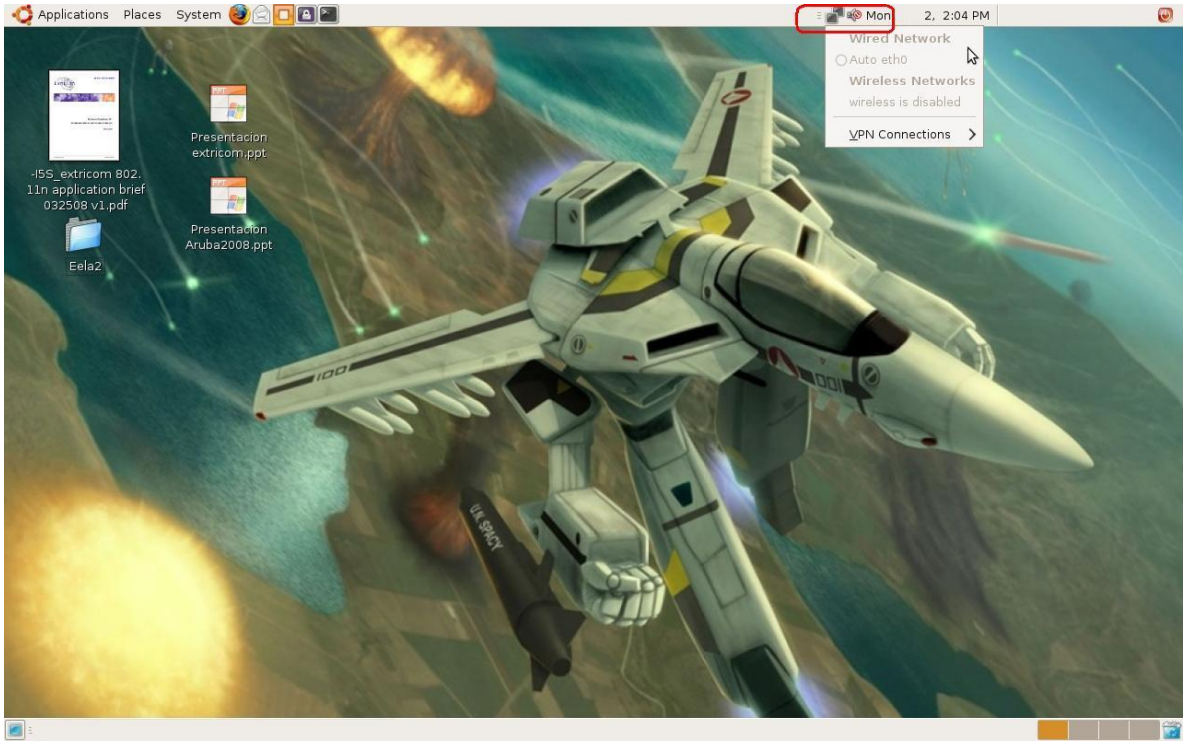
Apéndice D

Configuración de la Red Inalámbrica con Linux (Ubuntu)

La red inalámbrica es compatible con dispositivos inalámbricos que operan bajo los estándares 802.11b y 802.11g.

Esta guía ayudará a configurar su equipo de cómputo personal, laptop o PDA la conexión a la Red inalámbrica del Instituto de Física de la UNAM.

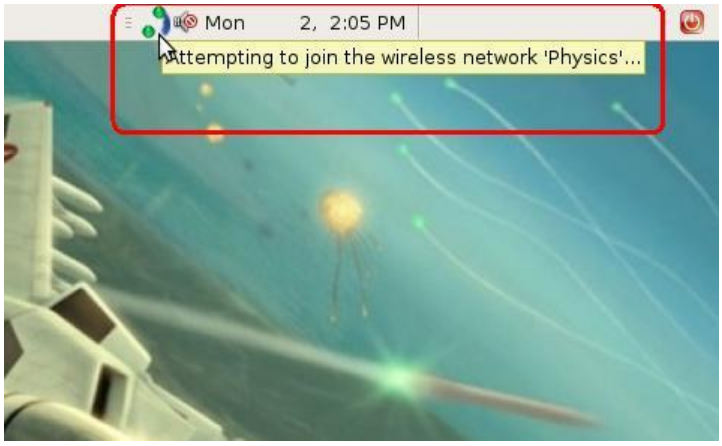
1. – Para usar la red, la tarjeta de red inalámbrica deberá estar activada en Ubuntu. Como se muestra en la siguiente figura.



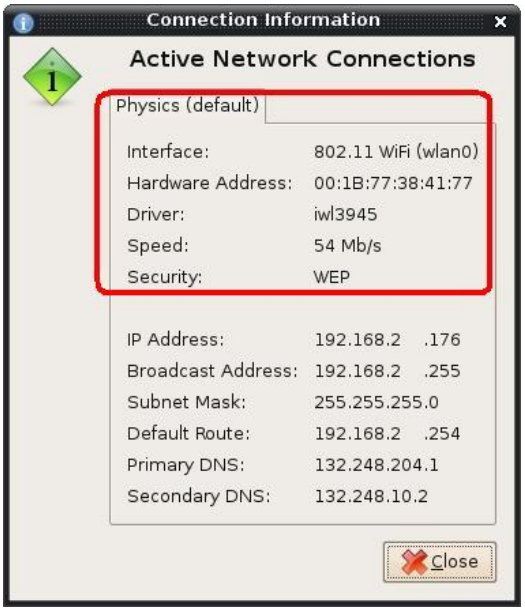
2. – Una vez que la tarjeta de red inalámbrica ya esta activa, damos click en el icono de **Status de Red** de Gnome Panel y seleccionamos **Connect to Hidden Wireles Network…**, como se muestra en la siguiente figura.

3. – Ingresamos el nombre de la red en el campo **Network Name** y en **Wireless Security** seleccionamos ***WEP 40/128-bit Key*** e ingresamos la clave **WEP** en el campo **Key** de la Red inalámbrica del Instituto, **WEP Index** la dejamos en 1 por defecto y **Authentication** queda como **Open System** y hacemos click en el botón **Connect**. Tal como se muestra en la siguiente figura.

4. – En estos momentos comienza hacer la conexión a la red, como se observa en la siguiente figura.



5. – Por último, nos indica que ya estamos conectados a la red inalámbrica. Para comprobarlo, solamente tendremos que verificar el estado de nuestra conexión. Como lo muestran las siguientes figuras.



Apéndice E

Configuración del Servidor DHCP, NAT y Firewall

```
#     $OpenBSD: dhcpd.conf,v 1.1 1998/08/19 04:25:45 form Exp $
#
# DHCP server options.
# See dhcpd.conf(5) and dhcpd(8) for more information.
#

# Network:      192.168.1.0/255.255.255.0
# Domain name:        my.domain
# Name servers:       192.168.1.3 and 192.168.1.5
# Default router:     192.168.1.1
# Addresses:          192.168.1.32 - 192.168.1.127
#
shared-network LOCAL-NET {
      option  domain-name "fisica.unam.mx";
      option  domain-name-servers 132.248.204.1, 132.248.10.2;

      subnet 192.168.2.0 netmask 255.255.255.0 {
            option routers 192.168.2.254;
                  range 192.168.2.1 192.168.2.160;
      }
```

Configuración Del Firewall

```
      #$OpenBSD: pf.conf,v 1.6 2002/06/27 07:00:43 fgsch Exp $
#
# See pf.conf(5) for syntax and examples
#
# replace ext0 with external interface name, 10.0.0.0/8 with internal
network
# and 192.168.1.1 with external address

ext_if = "xl0"
int_if = "xl1"

red_privada = "192.168.2.0/24"

redes_ifunam = "{ 132.248.29.0/24 132.248.8.0/24 }"

servicios_tcp = "{ 20 ftp 22 80 81 443 67 110 143 220 993 995 8991 1863}"

icmp_types= "echoreq"

nobloqueadas= "{ 192.168.2.180 192.168.2.179 192.168.2.178 192.168.2.177
192.168.2.176  192.168.2.175  192.168.2.174  192.168.2.173  192.168.2.172
192.168.2.171  192.168.2.170  192.168.2.169  192.168.2.168  192.168.2.167
192.168.2.166  192.168.2.165  192.168.2.164  192.168.2.163  192.168.2.162
192.168.2.161 192.168.2.144}"


#Opciones

set block-policy return
set loginterface $ext_if

# Normalize: reassemble fragments and resolve or reduce traffic ambiguities

scrub in all

# nat: packets going out through ext0 with source address 10.0.0.0/8 will
get
```

```
# translated as coming from 192.168.1.1. a state is created for such packets,
# and incoming packets will be redirected to the internal address.

nat on $ext_if from $int_if:network to any -> ($ext_if)

# rdr: packets coming in through ext0 with destination 192.168.1.1:1234 will
# be redirected to 10.1.1.1:5678. a state is created for such packets, and
# outgoing packets will be translated as coming from the external address.
#rdr on xl0 proto tcp from any to 132.248.29.200/32 port 8091 -> 192.168.2.91 port 80
#rdr on xl0 proto tcp from any to 132.248.29.200/32 port 8092 -> 192.168.2.92 port 80

rdr on xl0 proto tcp from any to 132.248.29.200/32 port 80 -> 192.168.2.80 port 8080

# filter rules
# the implicit first two rules are
#pass in log all allow-opts
#pass out log all allow-opts

# block all incoming packets but allow ssh, pass all outgoing tcp and udp
# connections and keep state
# log blocked packets

block log all

#loopback
pass quick on lo0 all

#Pasamos ssh solo para ifunam
pass in quick on $ext_if from $redes_ifunam keep state
pass in quick on $ext_if proto tcp from any to 132.248.29.200 port 81 keep state
pass in quick on $ext_if proto tcp from any to any port 81 keep state
pass in quick on $int_if proto tcp from $red_privada to any port $servicios_tcp keep state

#DNS
```

```
pass in quick on $int_if proto udp from any to any port domain keep state
pass out quick on $ext_if proto udp from 132.248.29.200/32 to any port
domain keep state

#ICMP
pass in inet proto icmp all icmp-type $icmp_types keep state

#Para la salida
pass out on $int_if from any to $int_if:network keep state
pass out on $ext_if proto tcp all modulate state flags S/SA
pass out on $ext_if proto {udp, icmp} all keep state

#pasamos todo para las fijas
pass out quick on $int_if from any to $nobloqueadas keep state
pass in quick on $int_if from $nobloqueadas to any keep state
pass in quick on $ext_if proto {udp, icmp} from any to 132.248.29.200 keep
state

#Correo electronico
pass in quick log on $int_if from $red_privada to 132.248.8.40 keep
state

#Para dirección general de bibliotecas
pass in quick on $int_if proto tcp from $red_privada to 132.248.9.25 port
4500 keep state
pass in quick on $int_if proto tcp from $red_privada to 132.248.67.3 port
8991 keep state
pass in quick on $int_if proto tcp from $red_privada to 132.248.9.4 port
8991 keep state
pass in quick on $int_if proto tcp from $red_privada to 132.248.67.65 port
8991 keep state

#Proyectos dgapa
pass in quick on $int_if proto tcp from $red_privada to 132.248.37.186 port
8443 keep state

#salva
pass in quick on $int_if from any to  132.248.8.50 keep state

#siesta
pass in quick on $int_if from any to  132.248.29.181 keep state
```

```
#conacyt
pass in quick log on $int_if from any to 148.207.1.0/24 keep state
```

Apéndice F

Ficha técnica de los equipos de la Red Inalámbrica

LINKSYS® by Cisco

cisco.

Less is More

Add wireless capability to your wired network and enjoy the convenience that comes when you eliminate cables. Add wireless devices to your network. With less wiring, you'll do much more.

Wireless Convenience
You've got the network – now enhance it with Wireless-G access up to 54 Mbps. Now it's easy to grow your network by adding computers, printers and other wireless devices, without stringing cables. Also compatible with Wireless-B devices. Reliable connectivity allows you to move your laptops, or set up your devices all around your home or office. Or add Access Points to two separate networks and create "cable-less cable" connectivity between them.

Easy Configuration
Push-button setup makes it simple to add devices to your new wireless network. Push the button on the Access Point and on any SecureEasySetup-enabled device to automatically create the wireless connection. Device and security configuration is a snap with the Browser-based configuration utility.

Complete Security
Work with confidence. Industrial-strength encryption helps keep your communications protected and private. Access filter lets you control who can get on your wireless network.

DATASHEET

Add high-speed Wireless-G access to your wired home or office network

Data rates up to 54Mbps in Wireless-G (802.11g) mode, and up to 11Mbps in Wireless-B (802.11b)

Push button setup feature makes wireless configuration secure and simple

Advanced wireless security: 128-bit WPA encryption and MAC filtering

www.linksys.com

Features

- IEEE 802.11g supports data rates up to 54Mbps
- Backwards compatible with existing IEEE 802.11b devices
- Easy wireless configuration with SecureEasySetup push button
- Supports WPA security and 64/128-bit WEP encryption
- Built-in web UI configuration for easy configuration from any Web-browser
- Firmware upgradable through web browser
- Supports Wireless Bridging, Wireless Repeater, MAC Address Filtering, and Event Logging
- Three-year warranty

cisco

Cisco Consumer Business Group
121 Theory
Irvine, CA 92617 USA

www.linksys.com

Specifications

Model	WAP54G
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Ports/Buttons	One 10/100 Auto-Cross Over (MDI/MDI-X) Port, Power Port, Reset and SES Buttons
Cabling Type	Category 5 (with RJ-45 connectors)
LEDs	Power, Activity, Link
Transmit Power	802.11g: Typ. 13.5 +/- 2dBm @ Normal Temp Range 802.11b: Typ. 16.5 +/- 2dBm @ Normal Temp Range
Security features	WPA, Linksys Wireless Guard (available in US and Canada only), WEP Encryption, MAC Filtering, SSID Broadcast Enable/Disable
WEP Key Bits	64/128-Bit

Environmental

Dimensions	7.32" x 1.89" x 6.65" (186 x 48 x 169 mm)
Weight	1.01 lbs (460 g)
Power	External, 12V DC
Certification	FCC, CE, Wi-Fi (802.11b and 802.11g)
Operating Temp.	32 to 150°F (0 to 40°C)
Storage Temp.	-40 to 185°F (0 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Package Contents

- Wireless-G Access Point
- Detachable Antennas
- Power Adapter
- Setup CD with User Guide
- Ethernet Network Cable

Minimum Requirements

- PC with 300MHz or Faster Processor
- 128MB RAM Memory
- Internet Explorer 5.0 or Netscape Navigator 6 or higher for Web-based Configuration
- CD-ROM Drive
- Windows 2000 or XP (to use the Setup Wizard)
- 802.11b Wireless Adapter with TCP/IP Protocol Installed
  or
  Network Adapter with Ethernet Network Cable and TCP/IP protocol Installed

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Specifications are subject to change without notice.

8120810A-ST

Model: **WAP54G**

www.linksys.com

Apéndice G

Fichas técnicas de los switches de la Red Local del Instituto de Física

VERTICAL HORIZON VH-2402S 10/100/1000 STACKABLE WORKGROUP SWITCH — **Data Sheet**

- **High-performance connectivity**
  - — 24 ports of 10/100 Mbps wire-speed connectivity and two option slots for expansion, as well as a dedicated management slot
  - — Configurable data queuing for priority traffic, per the IEEE 802.1p standard, supports time-sensitive applications such as voice and video streaming
  - — A 12,000 MAC address table allows the VH-2402S to be easily integrated into large enterprise networks
- **Stackable design**
  - — Stackable design allows up to four units to be connected via the VH-STACK interconnect module and cable
- **Simplified management**
  - — An entire stack can be managed as a single entity via an optional management agent
  - — IGMP snooping identifies and segregates unicast and multicast packet traffic to ensure an efficient utilization of the switch bandwidth
  - — Network management and configuration tasks are easily performed via local console port, web browser or any SNMP-based network management station including NetSight™
- **Standards-based VLAN support**
  - — Standards-based VLANs per the IEEE 802.1Q standard allow the VH-2402S to be seamlessly integrated into multivendor networks

An Ideal Enterprise Edge Switching Solution

The Vertical Horizon VH-2402S provides the features and performance required from a workgroup/desktop solution.

Wire-Speed Performance and Industry-Leading Features for Small and Medium Enterprises

The Vertical Horizon (formerly SmartSTACK) Fast Ethernet Stackable Switch (VH-2402S) provides 24 10/100 Mbps RJ45 ports and two option slots for expansion, as well as a dedicated management slot. Wire-speed performance and industry-leading features allow the Vertical Horizon Fast Ethernet Stackable Switch to integrate into small to medium-sized networks, and make it an ideal enterprise edge switching solution. Plug-and-play installation, advanced network management and standards-based switching features make the family of Vertical Horizon Fast Ethernet switches industry leaders in their class.

Vertical Horizon Fast Ethernet Stackable Switches provide all the features and performance required from a desktop or workgroup switching solution. The VH-2402S provides wire-speed 10/100Base-TX connectivity for the connection of high-performance workstations, file servers, desktop switches and shared access workgroup hubs. Two option slots for 100Base-FX and 1000Base-X uplink modules allow customers flexibility in their backbone connections and enable the stacking of multiple switches. The stack of switches can be managed as a single entity with the addition of the management agent anywhere in the stack.

The Vertical Horizon VH-2402S is ideally positioned as a high-performance workgroup switch suitable for supporting network-intensive applications and high-volume file transfers. It may also be used in wiring closet and desktop edge switching applications of large corporations where Gigabit Ethernet is the desired backbone technology. In addition, the VH-2402S can be used simply as a standalone switch.

ENTERASYS NETWORKS™

www.enterasys.com

VERTICAL HORIZON

PHYSICAL SPECIFICATIONS

Dimensions
6.4 cm (2.53") H x 44 cm (17.37") W x 28.5 cm (11.22") D

Weight
4.6 kg (10 lbs)

Interface Options
24 ports of 10Base-T/100Base-TX RJ45 and 2 option slots for uplinks and/or expansion modules

Processor
Winbond 78E516 (12.5 MHz)

Main Memory
8 MB

Buffer Memory
128k for 10/100 port; 2 MB for 1000 Mbps port

Flash Memory
2 MB

Address Table Size
12k entries

TECHNICAL SPECIFICATIONS

Performance Throughput Capacity
6.55 Mpps (single unit)/26.2 Mpps (4 high stack); all calculations based on 64 bytes per packet

Switching Bandwidth Capacity
8.8 Gbps

MTBF (predicted)
6 years

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature
0° to 50° C (32° to 122° F)

Operating Humidity
10% to 90% (non-condensing)

Operating Voltage
100 to 240 VAC

AGENCY AND STANDARDS SPECIFICATIONS

Safety
UL 1950, CSA C22.2 No. 950, 73/23/EEC, EN 60950, IEC 950

Electromagnetic Compatibility
FCC Part 15, CSA C108.8, 89/336/EEC, EN 55022, EN 61000-3-2,EN 61000-3-3, EN 50082-1, AS/NZS 3548, VCCI V-3

ORDERING INFORMATION

VH-2402S
Fast Ethernet stackable switch with 24-port 10/100 TX, 2 rear option slots, and dedicated management slot. (Must purchase 1 VH-SMGMT per standalone or 1 per stack)

Uplink Modules (PIMs)

VHIM1000-S1LX
1-port 1000Base-LX (Long Reach)

VHIM1000-S1SX
1-port 1000Base-SX (MMF, SC style connector)

VHIM100-S1SFX
1-port 100Base-FX (SMF, SC style connector)

VHIM100-S2MFX
2-port 100Base-FX uplink module (MMF, SC style connector)

Management and Interconnect Modules

VH-SMGMT
VH-2402S management module. (One required per stand-alone/one required per stack) Includes 5' female/female DB-9 serial console cable

VH-STACK
VH-2402S stack interconnect module with short 32 cm interconnect cable. (Must have one per unit within the stack)

Power Supplies

VH-1RDC
Single DC Redundant Power Supply Unit

Bundles

VH-S24MGMT
(1) VH-2402S and (1) VH-SMGMT

VH-S48BNDL
48-port 10/100 managed bundle. (2) VH-2402S, (1) VH-SMGMT, and (2) VH-STACK

VH-S72BNDL
72 ports 10/100: (3) VH-2402S (1) VH-SMGMT, and (3) VH-STACK

VH-S96BNDL
96 ports 10/100: (4) VH-2402S, (1) VH-SMGMT, and (4) VH-STACK

ENTERASYS NETWORKS™

enterasys.com

www.enterasys.com

VERTICAL HORIZON VH-8G GIGABIT ETHERNET STANDALONE WORKGROUP SWITCH

Data Sheet

- **1000 Mbps wire-speed switching**
  - Provides 8 ports of 1000 Mbps connectivity via fixed SC style connectors
  - Integrated ASIC design provides a total of 16 Gbps of internal switching fabric bandwidth and wire speed on all ports; throughput of over 12 Mpps
  - 8k MAC address table allows integration into large enterprise networks
- **Standards-based support**
  - Standards-based VLANs per the IEEE 802.1Q standard for seamless integration into multivendor networks
  - Supports IEEE 802.1Q MIB for easy management and configuration by NetSight
  - Complies with IEEE 802.1d and 802.3, to ensure compatibility with other standards-based networking products
  - Supports the IEEE 802.1Q VLAN specification for tag-based VLANs
  - Supports the IEEE 802.1p priority queuing specification for two priority queues
  - Supports 802.3x Flow Control in full duplex mode
- **Integrated network management**
  - Network management and configuration tasks are easily performed via local console port, web browser or any SNMP-based network management station
  - Supports port trunking on the 1000Base-SX ports
  - Supports 4 groups of RMON per port for network troubleshooting and monitoring
  - Port mirroring allows the connection of an RMON probe or data analyzer for advanced fault diagnosis
  - Supports TFTP download for easy in-band software upgrades
  - Provides broadcast throttling to reduce the number of broadcasts within a network

Standalone Switching for Small to Medium Enterprises

The Vertical Horizon VH-8G standalone switch allows high-performance, full-featured Gigabit Ethernet switching.

Gigabit Ethernet Connectivity for the Wiring Closet and Workgroup

The Vertical Horizon VH-8G is a high-performance standalone workgroup switch suitable for supporting network-intensive applications and high-volume file transfers. The VH-8G may be successfully deployed in wiring closet and desktop/workstation edge-switching applications where Gigabit Ethernet is the desired backbone technology.

With all the features and performance required from a desktop or workgroup switching solution, the Vertical Horizon VH-8G provides 8 SC ports of wire-speed 1000Base-SX connectivity to tie together high-performance workstations, file servers, desktop switches and shared access workgroup hubs.

Wire-speed performance on all ports and industry-leading features allow the Vertical Horizon VH-8G to integrate into small to medium networks as well as provide an ideal edge switching solution in larger enterprises. The VH-8G offers industry-leading price, performance and features along with ease of installation, and high reliability. Plug-and-play installation, advanced network management and standards-based switching features make the VH-8G Gigabit Ethernet Switch a leader in its class.

ENTERASYS NETWORKS™

www.enterasys.com

TECHNICAL SPECIFICATIONS

Processor
Winbond 78E516 (12.5 MHz)

Main Memory
8M bytes

Buffer Memory
1.25 Mb for each 1000Base-SX port

Flash Memory
2M bytes

Address Table Size
8k entries

Performance Throughput Capacity
12 Mpps (single unit) (all calculations based on 64 bytes per packet)

Switching Bandwidth Capacity
16 Gbps

MTBF (predicted)
6 years

PHYSICAL SPECIFICATIONS

Interface Options
8 fixed ports of 1000Base-SX SC MMF

Dimensions
6.4 cm (2.5") H x 44 cm (17.3") W x 28.5 cm D (11.2")
(height = 1.5 U; mountable in a standard 19 inch rack)

Weight
4.6 kg (10.2 lbs)

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature
0° to 50° C (32° to 122° F)

Operating Humidity
10% to 90% (non-condensing)

Operating Voltage
100 to 240 VAC

Power Consumption
80 watts

AGENCY AND STANDARDS SPECIFICATIONS

Safety
UL1950
CSA C22.2 No. 950
72/23/EEC
EN60950
IEC950

Electromagnetic Compatibility
FCC Part 15
CSA C108.8
89/336/EEC
EN55022
EN 61000-3-2
EN 61000-3-3
EN 50082-1
AS/NZS 3548
VCCI V-3

ORDERING INFORMATION

VH-8G
Gigabit Ethernet Standalone switch with 8 fixed SC MMF 1000Base-SX ports

VH-1RDC
Single DC redundant power supply unit

Lit. #9012120 01/01

ENTERASYS NETWORKS

enterasys.com

www.enterasys.com

SSR 2100

Performance

8.0 Gbps non-blocking switching fabric, 9.2 million pps routing throughput

Capacity

8 1000Base-SX ports supporting half or duplex operation

Management

Java-based CoreWatch, SPECTRUM

Technical

Switching Engine: Custom SmartSwitch Router ASIC

Buffer Memory: 3 MB per port

Routing Table Size: Up to 50,000 routes

Layer 2 Address Table Size: Up to 240,000 entries

Layer 3/4 Table Size: Up to 256,000 entries

Performance: 8.0 Gbps non-blocking switching fabric, 9.2 million pps routing throughput

Physical

Interfaces: 1000Base-SX

In-Band Management: Remote SNMP via CoreWatch and SPECTRUM

Out-of-Band Management: RS-232 and Telnet

MTBF (predicted): > 200,000 hours

Dimensions: 2.8" H x 17" W x18.5" D (7.1cm x 43.2cm x 47cm)

Weight: 22 lbs.

Environmental

Operating Temperature:
+5° to +40°C (41° to 104°F)

Non-Operating Temperature:
-30° to +73°C (-22° to 164°F)

Agency and Standards

Safety: Meets the requirements of UL1950, CSA C22.2 No. 950, EN60950, IEC950 and 72/73/EEC.

Electromagnetic Compatibility (EMC): Compliant with the requirements of FCC Part 15, CSA C108.8, EN555022, VCCI V-3/93.01, EN50082-1 and 89/336/EEC.

RFCs/MIBs: RFC 1213 - MIB-2
RFC 1493 - Bridge MIB
RFC 2233 - Interfaces MIB
RFC 1643 - EtherLike MIB
RFC 1163 - A Border Gateway Protocol (BGP)
RFC 1267 - BGP-3
RFC 1757 - RMON-MIB
RFC 1771 - BGP-4
RFC 1657 - BGP-4 MIB
RFC 1058 - RIP v1
RFC 1723 - RIP v2 Carrying Additional Information
RFC 1724 - RIP v2 MIB
RFC 1757 - RMON
RFC 1850 - OSPF v2 MIB
RFC 2096 - IP Forwarding MIB
RFC 1812 - Router Requirements
RFC 1519 - CIDR
RFC 1157 - SNMP
RFC 2021 - RMON2
RFC 2068 - HTTP

Fiber Type:
62.5mm MMF 50mm MMF

Transmit Power (minimum):
-9.5 dBm

Receive Sensitivity:
-17 dBm

Link Power Budget:
7.5 dB

Operating Range (Fiber Type, Modal Bandwidth, @850nm Range):
62.5 mm Fiber, 160 MHz/km, 2-220 Meters
62.5 mm Fiber, 200 MHz/km, 2-275 Meters
50 mm Fiber, 400 MHz/km, 2-500 Meters
50 mm Fiber, 500 MHz/km, 2-550 Meters

Product Ordering Information

Part No.	Description
SSR-2-GSX	SSR 2100 fixed configuration with 8 ports 1000Base-SX. Includes redundant power supplies, Router Services software and CoreWatch device management software.

For complete ordering information, including specific modules, contact your Cabletron representative at 603-332-9400 or contact your local authorized reseller. You may also visit our web site at ***www.cabletron.com/smartswitch-router****.*

About Cabletron

Cabletron Systems delivers high-performance networking solutions—award-winning hardware, software and services—to customers worldwide. With end-to-end solutions that offer a higher return on investment and a lower cost of ownership, Cabletron is the *e*-business communications specialist for the information age.

Your *e*-Business Communications Specialist™

Corporate	*Canada*	*Europe/Middle East/Africa*	*Asia Pacific*	*Latin America*	*Internet*
Tel (603) 332-9400 Fax (603) 337-2211	Tel (905) 673-8807 Fax (905) 673-9480	Tel 44-1635-580000 Fax 44-1635-44578	Tel 65-775-5355 Fax 65-776-3382	Tel 525-490-3400 Fax 525-652-9615	www.cabletron.com

Lit. #9011543 7/99

SmartSwitch Router 2100

SSR 2100

APPLICATION-AWARE SERVER LOAD-BALANCING SWITCH ROUTER

The SmartSwitch Router 2100 is a premier Layer 2, 3 and 4 application-aware switch router designed to deliver the functionality of the SmartSwitch Router to both workgroup and server farm environments. With the SmartSwitch Router 2100's Layer 4 switching capacity, application-level control can extend to the workgroup, while QoS and load balancing can be expanded to the server farm. In fact, with its 8.0 Gbps non-blocking switching fabric and 9.2 million pps routing throughput, the SmartSwitch Router 2100 offers one hundred times the performance of traditional routers at a cost comparable to Layer 2 switches.

The SmartSwitch Router 2100 provides eight 1000Base-SX ports which can operate in full duplex or half duplex mode. Each port may be configured as a switched or routed port.

Full-function IP/IPX routing enables the SmartSwitch Router 2100 to satisfy even the most traffic-intensive workgroup environments. More than 4,000 VLANs, 2,000 security filters and large per-port buffers provide the capacity to handle peak traffic to any workgroup. In addition, the SmartSwitch Router 2100 provides table capacities that are greater than any Layer 3 switching solutions available today, supporting up to 50,000 routes, 256,000 application flows and 240,000 Layer 2 MAC addresses.

The SmartSwitch Router 2100 can also be positioned as a Layer 2, 3 and 4 server load-balancing switch. Up to eight servers can be connected via 1000Base-SX connections, extending application control and providing the ability to load balance application flows across multiple servers.

- **Layer 4 application server load balancing, hardware-based network address translation and transparent web cached redirect**
- **Industry-leading performance—8.0 Gbps switching fabric delivering 9.2 Mpps switching and routing throughput**
- **Eight 1000Base-SX ports which can operate in full duplex or half duplex mode**
- **Layer 4 application control with packet forwarding based on Layer 4 application information**
- **Extensive QoS support with the ability to allocate application QoS to the desktop**
- **Security control via Access Control Lists which can be applied at Layer 2, 3 or 4 without compromising performance**
- **Full SNMP management via a Java-based device manager, CoreWatch**
- **Fully manageable with SPECTRUM**

CABLETRON SYSTEMS

www.enterasys.com

Apéndice H

Políticas de uso aceptable de la Red Inalámbrica del Instituto de Física

El instituto de Física, brindará a su comunidad académica y estudiantes asociados el servicio de acceso gratuito a Internet a través del uso de la Red Inalámbrica del Instituto de Física (WiFi), para la navegación en Internet y consulta de correo electrónico como un recurso para apoyar la labor académica y de investigación.

GENERALIDADES

Aplicación.
Las presentes políticas establecen los lineamientos generales a seguir para el acceso y uso de la WiFi y son aplicables a todos los usuarios del servicio proporcionado por la Secretaria Técnica de Cómputo y Telecomunicaciones del Instituto de Física (STCyT).

Emisión y modificación de normas.
La STCyT tiene la facultad de crear, modificar y emitir nuevas políticas de acceso a la WiFi, en consecuencia se reserva el derecho de hacerlo en cualquier momento, sin previa notificación a los usuarios.

De la información transportada en la Red.
La STCyT no controla ni es responsable del contenido y veracidad de la información que se transporta en la WiFi, en consecuencia los usuarios aceptan utilizar el servicio de comunicación sólo para enviar y recibir mensajes e información que sean apropiados.

El acceso al contenido publicado en Internet, archivos descargados, programas ejecutados desde Internet, mensajes recibidos y demás información que pueda estar en Internet, es susceptible de contener virus informáticos. Por lo anterior es responsabilidad del usuario ingresar sólo a sitios que considere seguros. La STCyT no se hace responsable por daños ocasionados a los archivos electrónicos que hayan sido modificados por virus informáticos.

Asignación del servicio.
Previo al cumplimiento de los requisitos que al efecto se establezcan, la STCyT configurara las conexiones de los usuarios para el acceso a la WiFi y generara un registro de estos para uso en la administración de la WiFi. Podrá solicitar la configuración del equipo a través de la STCyT al teléfono 56225001.

El servicio de acceso a la WiFi será proporcionado a la comunidad estudiantil y académica del Instituto de Física en forma gratuita.

Suspensión del servicio.
La STCyT podrá suspender o desactivar temporalmente sus servicios o cancelarlos definitivamente, cuando detecte que el usuario realiza usos prohibidos del servicio. A juicio de esta instancia se reactivará el servicio cuando se considere que el usuario no volverá a incurrir en una conducta prohibida del servicio.

Las siguientes son causas de suspensión temporal del acceso:

- Distribuir virus, gusanos u otro código malicioso de propagación automática y de forma involuntaria.

Las siguientes son causas de suspensión definitiva del acceso:

- Distribuir virus, gusanos u otro código malicioso de propagación automática y de forma voluntaria.
- Realizar actividades delictivas.
- Envío de mensajes no solicitados (spam).
- Atacar a otros usuarios por cualquier medio (negación de servicio (DoS), phishing, etc.).
- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.
- Cuando el usuario completó su ciclo escolar o dejó de ser académico o investigador universitario.

Disponibilidad del servicio.
El servicio de conexión a la WiFi estará disponible las 24 horas del día, todos los días del año. Salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio de Internet.

Configuración.
Los usuarios de la WiFi deberán contactar al personal de la STCyT para configurar sus sistemas.

Cobertura.
La WiFi tiene un alcance de operación en los siguientes edificios del Instituto de Física.

- Edificio Principal
- Biblioteca
- Auditorio
- Edificio Colisur
- Acelerador Van de Graff 2 MeVs
- Acelerador Van de Graff 5.5
- Laboratorio central de microscopia electrónica

Responsabilidad.

1. La STCyT es responsable de mantener la integridad y operación eficaz de los puntos de acceso a la WiFi, pudiendo realizar acciones de actualización y mantenimiento del servicio sin previa notificación a los usuarios.
2. La STCyT no se hace responsable por conductas difamatorias, obscenas u ofensivas que se realicen a través de los servicios que proporciona.
3. La STCyT es responsable de confirmar que los usuarios que soliciten el servicio sean estudiantes asociados al instituto, académicos, investigadores e invitados.
4. Es responsabilidad del usuario la seguridad física de su equipo, por lo que el Instituto de Física no es en ninguna forma responsable por robo o daños al equipo del usuario.
5. El usuario acepta y reconoce que la STCyT sólo provee de los recursos para acceder a los servicios que le son otorgados.
6. El usuario es responsable de la confidencialidad de las contraseñas de la conexión.

USOS PERMITIDOS.

Usuarios Autorizados

Son usuarios autorizados los que, previa autorización y cumplimiento de los requisitos correspondientes, tienen acceso a la WiFi y hacen uso de los servicios. Estos comprenden a los alumnos, académicos e investigadores del Instituto de Física de la UNAM.

Propósito de uso

En apego al quehacer de la UNAM y específicamente al Instituto de Física, el uso de los recursos para estos servicios deberá estar relacionado con las actividades académicas, de investigación y difusión de la cultura.

USOS PROHIBIDOS

Queda prohibido:

- El uso para generar ganancias monetarias personales o propósitos comerciales que no estén directamente relacionados con asuntos que la propia Universidad autoriza, difunde y solicita a la comunidad universitaria incluyendo en situaciones de contingencia.
- Enviar copias de documentos o inclusión de trabajos de otros en el correo electrónico como propios violando las leyes de derechos de autor.
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Extender el servicio de acceso a la WiFi a más equipos por medio de una sola conexión a la red inalámbrica (ej: por medio de NAT, túneles, conexión compartida, etc.)
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico (ej. antenas) más allá de los límites físicos de la Universidad. El acceso a la red inalámbrica se restringe al Instituto de Física.
- El uso del servicio para molestar, acosar, intimidar, amenazar a otros o atente contra la integridad de los usuarios o para interferir con asuntos propios de las autoridades Universitarias.

- El uso del servicio para violar las políticas de uso aceptable del correo electrónico
- Transgredir cualquier recurso computacional, sistemas o sitios de telecomunicaciones a los que no le está permitido acceder.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.

MONITOREO DE COMUNICACIONES

El usuario al momento de obtener el acceso a la WiFi, conoce y manifiesta su consentimiento para que la STCyT realice monitoreo en su conexión de acceso a la WiFi cuando lo juzgue necesario, únicamente con el propósito de mantener la integridad y operación efectiva de los puntos de acceso o cuando responda a un requerimiento de las autoridades administrativas o judiciales.

Requisitos para solicitud del servicio de acceso a Internet a través de la Red Inalámbrica (WiFi) del Instituto de Física (IFUNAM)

Los requisitos para obtener el acceso a la red son los siguientes:

Estudiantes:

- Ser estudiante y presentar su credencial vigente de estudiante asociado al IFUNAM.
- Contar con un equipo de cómputo portátil (Lap Top) que cuente con tarjeta de red inalámbrica estándar 802.11b y 802.11g.
- Solicitar una cita con el personal de la Secretaria Técnica de Cómputo y Telecomunicaciones (STCyT) para la configuración de su equipo de cómputo.

Académicos o investigadores:

- Ser académico o investigador y contar con el último talón de pago.
- Contar con un equipo de cómputo portátil (Lap Top) que cuente con tarjeta de red inalámbrica estándar 802.11b y 802.11g.
- Solicitar una cita con el personal de la Secretaria Técnica de Cómputo y Telecomunicaciones (STCyT) para la configuración de su equipo de cómputo.

Académicos, investigadores o estudiantes visitantes (que no formen parte de la comunidad UNAM):

- La persona responsable en el IFUNAM del estudiante o visitante deberá solicitar a la STCyT mediante una carta escrita la configuración del acceso a la WiFi.
- Contar con un equipo de cómputo portátil (Lap Top) que cuente con tarjeta de red inalámbrica estándar 802.11b y 802.11g.
- Solicitar una cita con el personal de la Secretaria Técnica de Cómputo y Telecomunicaciones (STCyT) para la configuración de su equipo de cómputo.

Red inalámbrica para foros, congresos y otros eventos académicos:

- Solicitar el servicio de acceso inalámbrico a la STCyT indicando nombre del evento, número de asistentes esperados, ubicación, duración y fecha del evento.
- Enviar la solicitud por lo menos 5 días antes de la fecha de inicio del evento.

NOTAS:

- Un usuario puede registrar uno o varios equipos los que usará con una misma contraseña, sin embargo un equipo no puede ser registrado por más de un usuario.

- El soporte para la conexión a la RIU se ofrecerá a través de los siguientes medios:
    - Al correo electrónico stec-if@fisica.unam.mx
    - Al teléfono 56.22.50.01 de la STCyT en el horario de 9:00 a 15:00 hrs.

Apéndice I

Costos de la Red Inalámbrica del Instituto de Física de la UNAM.

El costo total del proyecto fue de $ 72,144.10 pesos M.N., ver la siguiente tabla para conocer al detalle los equipos y materiales utilizados.

Cant.	Descripción	Marca	Modelo	Unidad	P. Unitario	Sub-total
23	Puntos de Acceso inalámbrico	LinkSys	WAP54G	Pza.	980.00	22,540.00
8	Bobina de cable UTP Cat 5e 350 MHz	Belden	1700A	Pza.	3,080.00	24,640.00
2	Caja con 100 Mts de cable AWG eléctrico calibre 14 blanco	Condumex	363122	Pza.	250.00	500.00
2	Caja con 100 Mts de cable AWG eléctrico calibre 14 rojo	Condumex	363123	Pza.	250.00	500.00
2	Caja con 100 Mts de cable AWG eléctrico calibre 14 negro	Condumex	363121	Pza.	250.00	500.00
23	Cajas para contactos dobles	Thorsman	7900-02001	Pza.	15.00	345.00
23	Contacto Dúplex polarizado con tierra física y con placa	Leviton	275-5262-I	Pza.	183.00	4,209.00
1	Lote de materiales varios (pijas, cinchos de plástico, velcro, etiquetas, etc)	Varios	Varios	lote	3,500.00	3,500.00
1	Computadora personal habilitada como servidor DHCP, NAT y Firewall	Ensamble	Ensamble	Pza.	6,000.00	6,000.00
					Sub-total	62,734.00
					I.V.A.	9,410.10
						$
					Total	**72,144.10**

No se consideran gastos de instalación de la infraestructura de la Red Inalámbrica debido a que la llevo a cabo el personal de la Secretaria Técnica de Cómputo y Telecomunicaciones del Instituto de Física de la UNAM.

Bibliografía

CARBALLAR, José A; *"Wi-Fi - Cómo construir una red inalámbrica"*

; Editorial. Alfaomega; 2da Edición, 2005.

CHRISTENSEN, Gerry; FLORACK, Paul G; DUNCAN, Robert; *"Wireless Intelligent Neetworking"*;; Editorial Artech House; E.U.A. 2001.

FRANCESCHETTI, Giorgio; STORNELLI, Sabatino; *"Wireless Networks"*

; Editorial Academic Press; E.U.A. 2006.

HELD, Gilbert; *"Securing Wireless Lan's"*

; Editorial WILEY; E.U.A., 2003.

LABOID, Houda; *"Wireless Ad Hoc And Sensor Networks"*

, Editorial WILEY; E.U.A 2008.

NEIL,Reid; RON, Seide; *"802.11 (WI-FI) Manual de Redes Inalámbricas*

; Editorial McGraw- Hill; 1ra. Edición (Español)2004.

PEIKARI, Cyrus; FOGIE, Seth; *"Wireless Maximum Security"*

; Editorial SAMS; 2da. Edición, E.U.A. 2003.

RAYA, José Luis; RAYA, Laura; *"Redes Locales*"

; Coedición Alfaomega - RaMa; 4ta. Edición, 2006.

STALLING, William; "*Wireless Communications And Networks"*

; Editorial Prentice Hall; E.U.A.2002.

KRICK, Edward; *"Introducción a la Ingeniería y al Diseño en la Ingeniería"*; Editorial Limusa; Edición Español México 2008.

Mesografía

Users POWER; Users POWER #41(2007); Artículo: *"Tu propia Red WI-FI"*; Autor: José Adrián Lligoña Bosch; MP editores; pp. 22 – 37.

Evolución de las redes inalámbricas

http://www.maestrosdelweb.com/principiantes/evolucion-de-las-redes-inalambricas/

Introducción a Wi-Fi (802.11 o WiFi)

http://es.kioskea.net/contents/wifi/wifiintro.php3

Redes Locales Inalámbricas

http://www.unincca.edu.co/boletin/indice.htm

Telefonía Celular

http://www.monografias.com/trabajos34/telefonia-celular/telefonia-celular.shtml

Wireless Deployment Technology and Component Overview

http://technet.microsoft.com/es-mx/library/bb457015(en-us).aspx

Fichas Técnicas de los Equipos.

www.enterasys.com

www.linksys.com

Instituciones Académicas.

www.unam.mx

www.fisica.unam.mx