UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

PROPUESTA DE UNA RED INALÁMBRICA BAJO EL ESTÁNDAR 802.11G Y SU SEGURIDAD EN LA ENEP ARAGÓN

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICO
ÁREA: ELÉCTRICA ELECTRÓNICA
P R E S E N T A :
VÍCTOR VIVEROS CHÁVEZ

ASESOR:
M. EN TEL. JOSÉ LUIS PÉREZ BÁEZ

MÉXICO 2005

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

DIRECCIÓN

VICTOR VIVEROS CHAVEZ
P r e s e n t e

Con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobado su tema de tesis y asesor.

TÍTULO:
"PROPUESTA DE UNA RED INALAMBRICA BAJO EL ESTANDAR 802.11g Y SU SEGURIDAD EN LA ENEP ARAGON."

ASESOR: Ing. JOSE LUIS PEREZ BAEZ

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 2 de septiembre de 2004.

LA DIRECTORA

ARQ. LILIA TURCOTT GONZÁLEZ

U.N.A.M. ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON
DIRECCION

C p Secretaria Académica
C p Jefatura de Carrera de Ingeniería Mecánica Eléctrica
C p Asesor de Tesis

LTG/AIR/rra

TRABAJO DE TESIS

Propuesta de una red inalámbrica bajo el estándar 802.11g y su seguridad en la ENEP Aragón

Nombre: Víctor Viveros Chávez

Octubre de 2004

Agradecimientos.

Ante todo agradezco la atención y paciencia ofrecida por mi asesor de tesis, el Ingeniero y Maestro José Luís Pérez Báez, que supo guiar en todo momento, este noble esfuerzo enfocando adecuadamente el trabajo de tesis a lo largo del desarrollo de esta. Sus sugerencias siempre fueron importantes para el avance de cada tema de la tesis.

Agradezco el conocimiento adquirido dentro de esta escuela y dentro de la UNAM dado que soy miembro de esta desde el nivel preparatoria desde el año de 1984. Por lo que mi perfil académico se lo debo a la UNAM como institución en general.

Agradecimientos a todos mis profesores que me impartieron clases, durante mi carrera de IME en la ENEP Aragón, con los que aprendí a enfrentar problemas desde otro punto de vista, tratando de buscar siempre una explicación al todo. Así mismo agradezco a la ENEP Aragón y a sus autoridades el haberme brindado un lugar dentro de esta institución.

Agradezco el apoyo brindado por mi familia en todo momento y el haber comprendido mi profundo interés por aprender cada día más, así como completar los requisitos que la UNAM requiere a todo profesional.

Por ultimo agradezco a mis compañeros que supieron tolerar mi punto de vista con respecto a algún tema en particular.

Dedico este trabajo de tesis a mi hermano que siempre estuvo conmigo y que siempre lo recordare, Javier Viveros Chávez, quien, a pesar de luchar día con día, sus sueños no se lograron. Descanse en paz.

Índice de contenido

Objetivo

Realizar un estudio y análisis de ingeniería para la instalación de una red inalámbrica con el estándar 802.11g, dentro de las instalaciones de la ENEP Aragón con la finalidad de proporcionar el acceso a los servicios de una red IP, incluyendo el acceso a la red mundial de Internet.

Para lograr lo anterior debemos conocer los fundamentos teóricos de las tecnologías asociadas a las redes inalámbricas WLAN, así como las medidas de seguridad asociadas a esta, para mantener la seguridad en la red LAN actualmente instalada.

La razón de este estudio es debido a que actualmente las tecnologías asociadas a la computación y redes de computadoras, son utilizadas ampliamente alrededor del mundo, en el ámbito empresarial, industrial, académico y domestico como un apoyo hacia el usuario final como los estudiantes, un gran numero de universidades ya utiliza esta tecnología como un medio mas para proveer de información a los alumnos. La instalación de una red inalámbrica permitirá:

Incrementar los medios y formas de obtener información.

Reducir la saturación de usuarios en los centros de cómputo

Proveer de acceso a Internet incluso fuera de los horarios ya establecidos

Aumentar el interés de los estudiantes por el estudio

Actualizar a la ENEP Aragón, en virtud que muchas universidades ya cuentan con este medio

Al ser un medio inalámbrico permitirá su utilización en áreas como la biblioteca, explanadas, salas salones, e incluso el auditorio solo por citar algunos ejemplos.

Hipótesis

Mediante un mejor entendimiento del estándar 802.11 y sus tecnologías asociadas como son tecnologías de radiocomunicaciones, de redes de computadoras y de seguridad, es posible implementar una red inalámbrica dentro de la ENEP Aragón con las medidas de seguridad necesarias para evitar ataques de hackers móviles en la red inalámbrica y en la red LAN, y a la vez permitir a los estudiantes el acceso a los recursos de la red inalámbrica y del Internet.

Introducción

Las universidades y empresas de los distintos sectores se están beneficiando de los desarrollos alcanzados en las redes WLAN. El desarrollo de las redes WLAN esta ligado a los demás desarrollos en comunicaciones inalámbricas, como son los radios de dos vías, sistemas de comunicación troncalizados, telefonía celular y enlaces de radiocomunicación para datos, por lo que es de suma importancia un entendimiento de la teoría de radiocomunicaciones y de redes de computadoras, y como estas se unen para formar dispositivos y sistemas WLAN. Las redes de computadoras al igual de otras tecnologías son estandarizadas y reguladas por organismos locales o internacionales, para permitir la interoperabilidad de los equipos en un mismo entorno. Es importante conocer a los organismos WLAN y mantenerse informados constantemente para conocer las modificaciones y/o actualizaciones relacionados con los sistemas WLAN y de esta manera hacer las actualizaciones al software y/o hardware asociado con las redes inalámbricas.

el presente documento, presenta el diseño de una red inalámbrica WLAN con el estándar 802.11g en las áreas mas concurridas de la escuela, para que sea usada por el sector estudiantil y académico de la escuela, brindando nuevos medios de obtención de información. Para brindar este servicio, además se implementaran mecanismos de seguridad con técnicas como protocolos de autenticación y encriptación.

Capitulo 1 Antecedentes

1.1 Antecedentes.

Las raíces de las comunicaciones inalámbricas digitales vienen desde 1940, cuando la telefonía móvil comercial empezó. Comparado con el violento pasó del desarrollo de hoy, puede parecer extraño que la comunicación inalámbrica móvil no haya progresado más en los últimos 60 años. Fueron muchas las razones para el retardo, pero las más importantes fueron la tecnología y la prudencia las autoridades reguladoras federales.

La revolución inalámbrica empezó solo después de que el descenso en los precios de los microprocesadores y dispositivos electrónicos digitales y analógicos, permitió que estos empezaran a ser disponibles para aplicaciones de radiocomunicación.

Existen diferentes definiciones para las comunicaciones inalámbricas entre las que encontramos son:

Comunicación por modulación y radiación de ondas electromagnéticas.

Un transmisor, un receptor o transmisor-receptor usado para comunicación vía ondas electromagnéticas.

Un término general aplicado al uso de ondas de radio.

La comunicación por radio así requiere una señal modulada dentro del espectro de radio, usando un transmisor y un receptor. La modulación incluye dos partes en su proceso de comunicación, actualmente llamados portadora y una señal con información (señal moduladora), generamos una onda portadora de alta frecuencia y entonces modulamos o variamos la corriente con la señal deseada a enviar. Actualmente existen varias técnicas de modulación.

Los dispositivos de radiocomunicación son instrumentos eléctricos, por lo que fue necesario un profundo entendimiento de la electricidad antes que los inventores pudieran producir un fiable y práctico sistema de radio. Algunos inventores y

científicos alrededor del mundo trabajaron en las diferentes partes enigmáticas de la radio. En una era de pobre comunicación e investigación poco sistemática, la gente duplico el trabajo de otros, minimizando los resultados de otros inventores, y frecuentemente eran mal interpretados los resultados que ellos mismos habían conseguido. Mientras se desconcertaban sobre los misterios del radio, muchos inventores trabajando, coincidieron en la generación de energía, telegrafía, iluminación, y por ultimo el teléfono.

1.1.1 Primeras investigaciones en electromagnetismo.

En 1723, el estadista norteamericano Benjamín Franklin hizo descender una corriente eléctrica por una nube tormentosa, sometió a prueba el pararrayos e ideo la manera de conservar la carga. El francés Charles Coulomb, encontró en 1785 la forma de medir la electricidad y el magnetismo. Finalmente en 1795 el físico italiano Alessandro Volta consiguió producir y almacenar electricidad. El descubrimiento de la electricidad abrió múltiples caminos para obtener inventos más avanzados como el telégrafo. Entre los experimentos más importantes que condujeron a su invención, se encuentran el del físico danés Hans Ch. Oersted, quien descubrió la relación entre la electricidad y el magnetismo, cuando todavía se creía que eran dos fenómenos distintos. Estableció por primera vez que la corriente no circula sola por un alambre sino que va acompañada de un invisible campo de fuerzas magnéticas.

En 1729, el inglés Stephen Gray descubrió la manera de transmitir electricidad por frotamiento de varillas de vidrio.

En 1830 un profesor americano de ciencias, Joseph Henry transmite la primera señal eléctrica práctica. En poco tiempo Henry había inventado el primer electromagneto práctico. El también había pensado de forma similar en relación a la inducción, pero el no lo publico antes que Faraday.

En 1837 Samuel Morse invento el primer telégrafo práctico, patentándolo en el año de 1838. El telégrafo pronto fue utilizado de forma comercial primero en todos los

estados unidos de Norteamérica y después el resto del mundo, remplazando a los medios tradicionales de mensajeria.

En 1843 Michael Faraday (1791-1867) empezó una investigación intensiva, para saber si el espacio podía conducir electricidad. En abril de 1846 reportó sus descubrimientos, en el discurso llamado "pensamientos en vibraciones de rayos". Él continúo trabajando en esta área por varios años, con investigadores y académicos siguiendo de cerca sus descubrimientos y teorías.

El descubrimiento que revolucionó la comunicación telegráfica y telefónica fue la aplicación de la radioelectricidad a estos dos tipos de sistemas de telecomunicaciones a fines del siglo XIX, mismo que permitió la transmisión telegráfica inalámbrica, facilitó la comunicación entre largas distancias y ahorro la construcción de extensas redes de hierro galvanizado o cobre. Hasta el siglo referido, prevalecía aun la idea newtoniana de la luz como emisión de partículas de un foco emisor; cuando se supero ese paradigma de la física, aparecieron descubrimientos sucesivos que sentaron las bases para la telegrafía y la telefonía sin hilos. El físico James C. Maxwell formuló la teoría electromagnética de la luz señalando su carácter ondulatorio, es decir su transmisión a través de ondas invisibles para el ojo humano. Estableció que los campos eléctrico y magnético actuando juntos, producían un nuevo tipo de energía llamada radiación electromagnética.

James Clerk Maxwell (1831-1879), reflexionaba constantemente sobre los descubrimientos de Faraday, trasladando e interpretando estos resultados de campo en un conjunto de ecuaciones matemáticas.

Maxwell a menudo movía estas ecuaciones en muchos papeles que él publicaba sobre electricidad y magnetismo. Científicos sabían que la luz era una onda pero ellos no sabían como estaba hecha. Maxwell se lo imaginaba. En 1864 Maxwell libera sus notas "teoría dinámica del campo electromagnético" el cual incluía la luz,

electricidad y magnetismo, eran todos relacionados, todos trabajaban mano a mano, y todos estos fenómenos electromagnéticos viajaban en ondas.

Maxwell encontró información adicional. Si la electricidad variaba rápidamente en cantidad, entonces las ondas electromagnéticas podían ser producidas, ellas se radian en ondas a puntos distantes. Al menos, así decía él. No había un método todavía para probar que "otras radiaciones" existían, para demostrar que otras ondas ocurren como la luz.

Las ecuaciones de Maxwell establecieron que la radiación se incrementaba dramáticamente con la frecuencia, esto es, muchas más ondas de radio son generadas a frecuencias altas que en baja frecuencia, dando la misma cantidad de potencia. La experimentación con la generación de ondas de alta frecuencias empezó así, de esta manera, esta no fue una tarea fácil.

1.1.2 Primeros descubrimientos de radio

Sobre los siguientes treinta años, diferentes inventores, incluyendo a Thomas Alba Edison, experimentaron con varios esquemas de inducción. Los sistemas más exitosos fueron montados a bordo de trenes, donde un alambre en la parte alta de carro de pasajeros podía comunicarse por inducción con un telégrafo alambrado a lo largo del camino.

Las conclusiones de Maxwell de 1864 fueron distribuidas alrededor del mundo y crearon sensación. Pero no fue hasta 1888 que el profesor Heinrich Hertz (1857-1894) de Bonn Alemania, pudo de manera confiable producir y detectar ondas de radio.

El 22 de noviembre de 1875 mientras trabajaba en un telégrafo acústico, Thomas Alba Edison, noto una fuerza extraña generada por lo que el llamo "vibración magnética", esta fuerza extraña así llamada por el, decía, podía sustituir alambres y cables en los medios de comunicación.

De 1879 a 1886 David Hughes, descubrió las ondas de radio, el trabaja bajo contrato para la Western Union el fue el considerado por muchos como el inventor de primer micrófono práctico, un dispositivo que hizo realidad el teléfono.

El 22 de Febrero de 1880, Alexander Gram. Bell y su primo Charles Bell se comunicaron con un foto-fono, un invento concebido por Bell, este dispositivo transmite voz sobre haces de luz

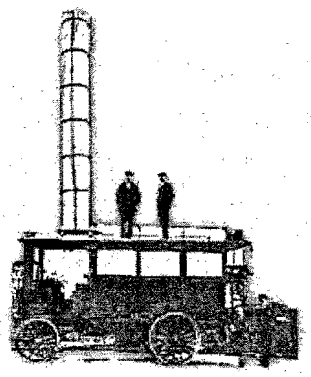


Figura 1.1.2-1 Primer móvil inalámbrico

En 1888 el alemán Heinrich Hertz (1857-1894) probó las predicciones de Maxwell que la electricidad podía viajar en ondas a través de la atmósfera. Con el descubrimiento de estas ondas que viajan por el espacio, se ideó la forma de producirlas y recibirlas a través de aparatos que aprovecharan los fenómenos eléctricos que la física había descubierto. A diferencia de Hughes, los extensivos y sistemáticos experimentos en ondas de radio conducidas por Hertz, fueron reconocidos y validados por inventores alrededor del mundo.

Algunos más como Edison, invento el bulbo incandescente de luz, mientras que Marconi ciertamente estableció el primer exitoso y práctico sistema de radio. Empezando en 1894 con sus experimentos eléctricos, y continuando hasta 1901 cuando su sistema de radio telégrafo envió señales cruzando el océano Atlántico. Guillermo Marconi consiguió el 2 de junio de 1891 una patente para la telegrafía sin

hilos. Marconi se había concentrado en la idea de utilizar dichas ondas para transmitir señales a través del espacio. Los barcos fueron las primeras plataformas móviles inalámbricas. En 1901 Marconi puso un radio a bordo de un camión movido por vapor (ver Figura 1.1.2-1 Primer móvil inalámbrico), esto produjo el primer móvil inalámbrico en tierra (transmitiendo datos por su puesto y no voz).

Lo que posibilitó la introducción de radiotelefonía en los hogares fue la transición, dentro del campo de las ondas electromagnéticas, del telégrafo al teléfono.

1.1.3 Inicios de la comunicación móvil.

Los receptores de radio con detectores de cristal sensitivos y económicos, aparecieron al principio de 1904, y fueron usados por muchos amateurs hasta principios de los treintas, cuando las válvulas de vació remplazaron a los cristales. Desde 1910 parece que Lars Magnus Ericsson y su esposa Hilda regularmente trabajaban en el primer teléfono de carro. Si este fue el hombre que fundo Ericsson en 1876. Aunque él estaba retirado a la agricultura en 1901, y al parecer, su esposa Hilda quería recorrer el campo justamente con el nuevo artilugio, el carro sin caballos. Lars fue renuente a ir pero muy pronto se dio cuenta que él podía tomar el teléfono a lo largo del trayecto. El acceso no fue por radio, por su puesto, pero era un intento de movilidad, en su lugar, fueron dos largos bastones, como cañas de pescar, manejadas por Hilda. Ella debía engancharlos en un par de alambres de telefonía, buscando un par que estuviera libre, cuando estos fueran encontrados, Lars Magnus accionaba la manivela del dinamo del teléfono, el cual producía una señal al operador en la cercana oficina de intercambio ver Figura 1.1.3-1 Primer teléfono móvil alambrado. Hasta los años 20s, los sistemas de radio móvil principalmente hacían uso del código Morse.

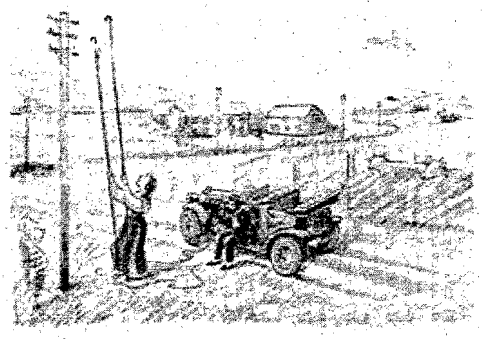


Figura 1.1.3-1 Primer teléfono móvil alambrado

1.1.4 El primer radio teléfono montado en carro.

La policía y los servicios de emergencia manejaban los sistemas pioneros de los radios móviles. Los equipos en todos los casos eran principalmente experimentales, con sistemas prácticos no implementados hasta los años 40´s y sin interconexión con los sistemas de telefonía.

Los laboratorios Bell reclaman haber inventado el primer radio teléfono de voz móvil de dos vías en 1924 ver Figura 1.1.4-1 Primer teléfono de voz móvil.

La F.C.C. dio prioridad a los servicios de emergencia, agencias gubernamentales, compañías utilitarias y de servicios pensando ayudar a la mayoría de la gente. Usuarios de radio como servicios de taxi o camiones de remolques requerían un pequeño uso del espectro para sus negocios. En comparación la radio telefonía usaba grandes bloques de frecuencias para servir solo a algunas gentes. La F.C.C., no permitió canales privados de radio telefonía hasta después de la segunda guerra mundial.

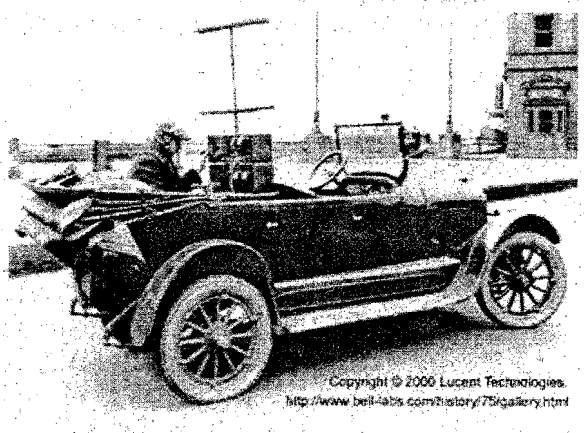


Figura 1.1.4-1 Primer teléfono de voz móvil

Aquí llegamos a un punto importante, dado que ahora no solo existe radiocomunicación móvil convencional sino también radiocomunicación celular. Donde la radiocomunicación móvil celular define nuevas técnicas de operación de los dispositivos móviles con sus respectivas radio bases.

En telefonía móvil un canal es un par de frecuencias. Una frecuencia para transmitir y una para recibir, para completar la ruta completa de comunicación. Suena bastante simple para acomodar. Todavía el espectro de radio es extremadamente saturado. Radios ineficientes contribuían a la saturación, usando un ancho de banda de 60 Khz. para enviar una señal que puede ahora ser enviada con 10 Khz. o menos.

Sensitivos, voluminosos, alto consumo de corriente, los radios con tubos serían remplazados en los siguientes 10 o 15 años con unidades de bajo consumo sumamente pequeños. Por los fines de los años 40´s y la mayoría de los 50´s la mayoría de los fabricantes de radios preferían tubos.

Equipos de radio móvil o sistemas de comunicación de negocios servían a remolques, taxis y camiones de servicios, donde un despachador se comunicaba a los móviles desde una estación base central. Estos sistemas de radio para negocios

eran y continúan en estos días siendo simples, comunicación de dos vías, uno habla mientras los demás escuchan en un tiempo dado.

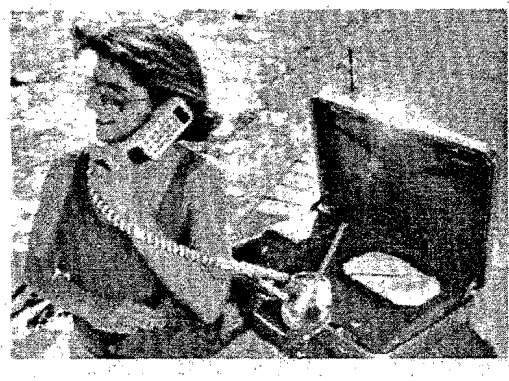


Figura 1.1.4-2 Primer móvil celular portable

Las frecuencias limitadas no eran permitidas para radio telefonía, solo el gobierno e instituciones podían utilizarlas, y fueron demandas ampliamente por el público.

Las primeras unidades de radiocomunicación portables eran realmente grandes y pesadas. Llamadas transportables o de equipaje, ver Figura 1.1.4-2 Primer móvil celular portable, pocos eran atractivos como las hechas por la empresa Spectrum Cellular Corporation. Oki también produjo un modelo de maletín.

Hasta hace no más de 24 años empezaron a surgir a nivel mundial estándares de telefonía celular como AMPS, años después surgieron tecnologías digitales como CDMA IS-95 y TDMA IS-136. Siendo su principal aplicación la voz y en pequeñas proporciones datos a muy baja velocidad.

Ahora disponemos de tecnologías como el GSM con mejores desempeños en la transmisión de datos. Pero paralelo al desarrollo de la telefonía celular digital surgen las redes inalámbricas para el manejo exclusivo de datos.

1.2 Inicios de las WLAN

En los años 80´s empezaron a surgir equipos para datos, teníamos sistemas DSSS (secuencia directa/espectro disperso) a 860 kbps. Estos fueron fáciles de desarrollar y básicamente no requerían de reglas o licencias. Esto fue bueno pero dado que no había reglas sobre estos, hacia que los equipos de distintas marcas fueran incompatibles.

Paro los años 90´s estas cosas cambiaron. LAN inalámbricas se movieron a la banda de 2.4 GHz el cual fue al menos utilizado por sistemas DSSS o FHSS con desempeños de 1 a 2 Mbps.

En 1992, el IEEE empezó a hacer el borrador del 802.11 y en julio de 1997 el DSSS en la banda de 2.4 GHz fue ratificado a 1 y 2 Mbps. En septiembre de 1999, el IEEE ratifico el estándar 802.11a (5 GHz a 54 Mbps) y posteriormente el 802.11b (2.4 GHz a 11 Mbps) y el año pasado (2003) fue ratificado el estándar 802.11g el cual combinara lo mejor de 802.11a y 802.11b (2.4 GHz a 54 Mbps) y es compatible con el estándar 802.11b.

Roaming es una tecnología conveniente de WLAN los usuarios pueden acceder los recursos de la red sin la necesidad de conectarse físicamente a la red. Tantos usuarios como puedan estar dentro del área de cobertura de un punto de acceso, son los que podrán ser usuarios móviles.

Las redes WLAN proporcionan simplicidad a los usuarios, dado que estos disponen de los mismos recursos que un equipo alambrado en la red.

La instalación de las redes inalámbricas es normalmente fácil y rápida. No necesita de instalar cables a través de los muros o por arriba de los techos. Las redes inalámbricas van donde otras redes no pueden. Como nota de esto se dice que la NASA empleara redes WLAN para la exploración del planeta Marte.

Las redes WLAN pueden ser diseñadas para ser simples o muy complejas. Estas redes pueden soportar amplios números de usuarios y cubrir amplias áreas físicas mediante la adición de puntos de acceso para extender la cobertura.

El costo de instalación y mantenimiento de una red inalámbrica es en promedio bajo en comparación con la instalación y mantenimiento de una red alambrada. El costo inicial de alambrar un edificio o construcción es eliminado así como el costo de mantenimiento de este. Mover adicionar y cambiar es mas simplificado que en una red alambrada tradicional.

Las redes WLAN es la culminación de dos campos tecnológicos fascinantes, las redes de computadoras y la radio comunicación, ambas tuvieron que pasar por muchos cambios tecnológicos para poder llegar a lo que ahora conocemos como WLAN. Existe mucha polémica alrededor de esta tecnología, donde algunos afirman que podría ser la competencia de las redes de telefonía móvil y otras afirman que van a ser tecnologías aliadas para un fin común. Lo que si es cierto es que esta tecnología esta evolucionando constantemente y que además llego para quedarse.

1.3 Avances que contribuyeron a las radiocomunicaciones

La evolución de las redes de telecomunicaciones ha dependido del desarrollo de materiales semiconductores, la explotación del espectro radioeléctrico y el diseño de artefactos para generar y recibir radiaciones. Por ello, las telecomunicaciones son fruto de los cambios de la física, desde antes de la primera revolución industrial, aunque su desarrollo se hace mas presente desde el siglo XIX. Los aportes científicos y tecnológicos de la electrónica, microelectrónica, ciencia de materiales el espacio, óptica, y cibernética entre otros. Ya en el siglo XX incidieron directamente en el perfeccionamiento de las primeras redes y la diversificación de servicios.

El primer paso para lograr que la radiotelegrafia se convirtiera en radiotelefonía fue el invento del bulbo, y el micrófono. El micrófono se necesitaba para poner los sonidos en el aire (el micrófono actúa como un traductor de señal al recibir ondas

sonoras y convertirlas en ondas eléctricas), y el bulbo para amplificarlos y enviarlos hacia la antena.

Con estos adelantos, para 1908 fue posible sostener una conversación radiotelefónica a una distancia de 500 kilómetros, aproximadamente.

Los científicos contribuyeron a hacer realidad este medio de telecomunicación, quizás nunca pensaron que sus descubrimientos serian la base para el despegue y desarrollo posterior de grandes industrias lucrativas como la telefonía sin hilos, la navegación marítima, la transportación aérea, la comunicación por satélite y la conquista espacial.

Con la radiocomunicación, la telegrafía sin hilos se convirtió en el medio por excelencia para las comunicaciones internacionales y prácticamente confino a las redes de cable a uso local.

La telefonía es el medio de telecomunicación que más impacto ha tenido sobre la humanidad. Es un sistema que sé utiliza para la transmisión de la voz, sonido, imágenes, video y datos a distancia, por acción de corrientes eléctricas y ondas electromagnéticas.

La búsqueda de nuevas tecnologías de comunicación durante más de un siglo, se ha concentrado fundamentalmente en perfeccionar a este medio de telecomunicación por excelencia.

Su disponibilidad a costos relativamente bajos y fácil manipulación, lo convirtieron no solo en un implemento auxiliar de la vida cotidiana sino en un medio indispensable para la economía, la política y la cultura.

En los últimos años, las modernizaciones del sistema telefónico y las telecomunicaciones avanzan a pasos agigantados también gracias a la explotación tecnológica de los enlaces de radio. Aunque los enlaces de radio se empezaron a

utilizar desde la segunda guerra mundial, fue hasta hace dos décadas que inicio su cabal aprovechamiento.

Los avances de la telecomunicación inalámbrica están asociados al descubrimiento y explotación de la radiación electromagnética, que es energía radial con forma de ondas invisibles que se propagan por el espacio y la materia. La radiación es óptimamente utilizada para transmisiones electrónicas, dentro del espectro radioeléctrico en diferentes longitudes e intensidad.

Las microondas son ondas de radio generadas a frecuencias muy altas. A diferencia de la longitud de 3200 metros que alcanzan las ondas en las frecuencias del espectro, las microondas obtienen longitudes que van de los 100 centímetros a un milímetro. Además de usarse en la radiodifusión, radiotelegrafia, televisión, satélites, tiene aplicaciones en intervenciones quirúrgicas, laboratorios de física, hornos de uso industrial y domestico, combaten plagas, etc.

La emisión de microondas para telecomunicaciones se realiza a través de torres de transmisión, instaladas en línea visual en puntos elevados a distancias entre 30 y 50 kilómetros, pero también existen ciertas bandas de frecuencia que soportan obstáculos tales como construcciones y pequeños cerros en función de la frecuencia y de la potencia de la señal así como de condiciones atmosféricas, se enfocan en haces direccionales, utilizan repetidores para reforzar las señales periódicamente.

Para prever la explotación irracional del espectro y el uso indiscriminado de equipo, se han establecido normas técnicas internacionales para controlar el uso de frecuencias por los particulares. En épocas de guerra los sistemas de radio son cruciales por la alta capacidad de transmisión y por la ventaja de no tener que emplear cables conductores.

En la primera guerra mundial se uso el radioteléfono trasatlántico para las comunicaciones con los barcos navieros y mercantes, después que los cables que unían a Alemania y Gran Bretaña fueron cortados al iniciar el conflicto en 1914.

Durante la segunda guerra mundial, la tecnología de microondas sirvió de base para el radar. Las primeras instalaciones de radar eran limitadas y poco confiables; conforme los militares exigieron mejor definición y certeza hacia el final de las hostilidades, los tecnólogos fabricaron equipo que permitía blancos precisos, usando las partes más altas del espectro.

Durante la segunda Guerra mundial los trabajos de la telefonía móvil civil y comercial pararon, pero la intensiva investigación y desarrollo fue para uso de las fuerzas militares. Mientras el radar fue quizás el más publicado, mientras otros productos eran realizados bien. El primer radio portátil de dos vías FM, el Walkie-talkie radio de mochila a la espalda fue diseñada por Dan Noble de Motorola. Y el Handie-talkie, el radio de mano se volvió un articulo vital para las comunicaciones en el campo de batalla a través de Europa y el pacifico sur durante la segunda guerra mundial.

1.3.1 Breve historia de los semiconductores

En el año de 1880 Edmond Becquerel, Ferdinand Braun y Michael Faraday, encontraron que ciertas sustancias, después conocidas como semiconductores, tenían características eléctricas útiles e inusuales.

En el año de 1920, es inventado el amplificador de tubo de vació por Irving Laymuir y Lee DeForest. Un componente esencial para los radares, la radio y las computadoras.

En septiembre de 1939, Jack Scaff y Henry Theurer, investigadores de los laboratorios Bell en Holmdel NJ, descubren las regiones positivas (tipo P) y negativa (tipo n) en el silicio.

El 29 de Diciembre de 1939, William Shockley, físico de los laboratorios Bell, conceptualizo la posibilidad de desarrollar un amplificador usando materiales semiconductores.

De 1946 al año de 1957 es fabricado y usado ampliamente el tubo de vació.

En 1946, el primer circuito en tarjeta, un producto de la guerra tecnológica, fue disponible comercialmente. Observe la pequeña tarjeta en la parte inferior de la derecha de la Figura 1.3.1-1 Primer circuito integrado. Tardarían muchos años antes de que tales tarjetas pequeñas fueran de uso común. Estos pequeños tubos fueron llamados "tubos de bellota" y fueron generalmente usados en equipos de baja potencia. Carros montaban teléfonos móviles usando tubos grandes y circuitos.

El 16 de diciembre de 1947, es inventado el punto de contacto para los dispositivos semiconductores, consistiendo de germanio, tiras de oro, aisladores y alambres.

El 23 de Diciembre de 1947, el transistor experimental es demostrado a los administradores de los laboratorios Bell, es usado para demostrar la amplificación de una señal de voz sobre un altavoz. Una enorme investigación y desarrollo es hincada para hacer el invento práctico, confiable y lo suficientemente barato para su fabricación

En diciembre de 1947 D.H. Ring de los laboratorios Bell articulo el concepto celular para telefonía celular en un memorando interno, como autor Ring y asistido por W.R. Young. Mr Young después renombro estos elementos como eran conocidos: una red de pequeña área geográfica llamadas células, un transmisor de baja potencia en cada una, el trafico celular controlado por un switch central, reutilización de frecuencias por diferentes células y así sucesivamente.

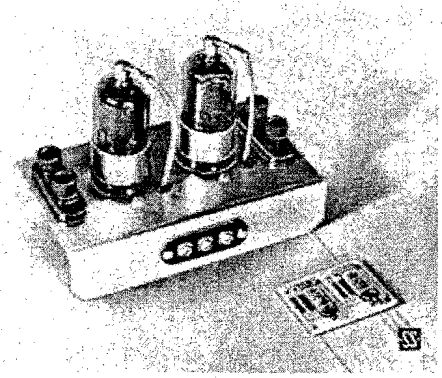


Figura 1.3.1-1 Primer circuito integrado

En el año de 1951 los científicos de los laboratorios Bell Gorden Teal y J.B. hacer crecer una pequeña pieza de cristal de germanio, el cual fue esencial para el desarrollo de el nuevo transistor de juntura.

En el año de 1951 los laboratorios Bell desarrollaron el transistor de juntura, el cual es más confiable y efectivo que el transistor de punto de contacto, comienza la fabricación del primer transistor, empezando en la planta de Allentown de Western Electric, que ahora es parte de Lucent Technologies.

1952, se otorga licencias a compañías para la fabricación del transistor, científicos de los laboratorios Bell, enseñan a la comunidad industrial como crear aplicaciones usando el nuevo dispositivo.

1953, científicos de los laboratorios Bell refinan sus técnicas para crear obleas de silicio puro para ser usados como material semiconductor.

1954, Carl J. Frosch y L. Derick de los laboratorios Bell descubren que una capa de dióxido de silicio podía ser usada como mascara de la superficie de silicio y permitiendo colocar de forma precisa las impurezas necesarias para crear las junturas necesarias, técnica que después seria usada en los circuitos integrados.

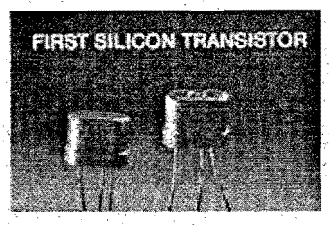


Figura 1.3.1-2 Primer transistor

En 1954, Texas Instruments fue la primera compañía en iniciar la comercialización de la producción de transistores de silicio en lugar de Germanio. El Silicio aumentaba la potencia de salida mientras operaba a bajas temperaturas permitiendo la miniaturización de componentes electrónicos. El primer transistor comercial también fue producido en 1954 por TI, ver Figura 1.3.1-2 Primer transistor.

En el mismo año Motorola produce su primer producto transistorizado comercial: un radio de automóvil. "es pequeño y mas durable que las modelos previos y demanda menos energía. Un radio de totalmente transistorizado, es considerado el mas confiable de la industria."

1956, los científicos de los laboratorios Bell Bardeen, Brattain, y Shockley, reciben el premio Nóbel de física por sus trabajos relacionados con el transistor.

1958 la compañía Cray introduce la primera supercomputadora completamente transistorizada.

En 1965 la miniaturización permitió a la telefonía móvil realizar sus grandes logros para la fecha, al otro lado del océano los japoneses estaban operando un teléfono de radio móvil convencional y estaban viendo por un mejor futuro.

1966 las técnicas de fabricación permitían realizar circuitos integrados con 100 a 1000 transistores. (MSI).

1969, las técnicas de fabricación permiten realizar circuitos integrados con 1000 a 10000 transistores (LSI).

En 1971 Intel introdujo su primer microprocesador, el 4004 ver Figura 1.3.1-3. Diseñado originalmente para calculadoras de escritorio, el microprocesador fue pronto mejorado y rápidamente puesto en todos los campos de la electrónica incluyen teléfonos celulares. El original hacia 4000 operaciones por segundo. De acuerdo con la emisión de "wired magazine" de Junio del 2001, Gordon Moore describia el microprocesador como "uno de los productos mas revolucionarios en la historia de la humanidad." Motorola también hizo mucho los tiempos pioneros de los microprocesadores y el campo de los semiconductores.

1973, Motorola introduce el radio teléfono celular portable, el precursor del moderno teléfono celular.

1975, las técnicas de fabricación permiten realizar circuitos integrados con 10000 a 100000 transistores. (VLSI)

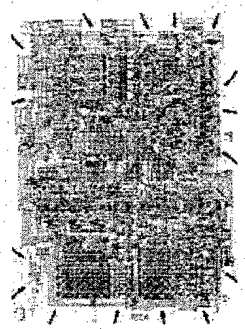


Figura 1.3.1-3 Primer microprocesador

1980, para esta fechas los circuitos integrados rebasan los 100000 transistores por chip. (ULSI).

En 1983 Texas Instruments introdujo su procesador de señal digital simple, con mas de 5 millones de operaciones por segundo ver Figura 1.3.1-4. Aunque no el primer en hacer chips DSP, Lucent clama esta distinción en 1979.

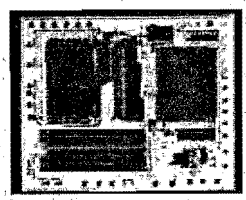


Figura 1.3.1-4 Primer DSP

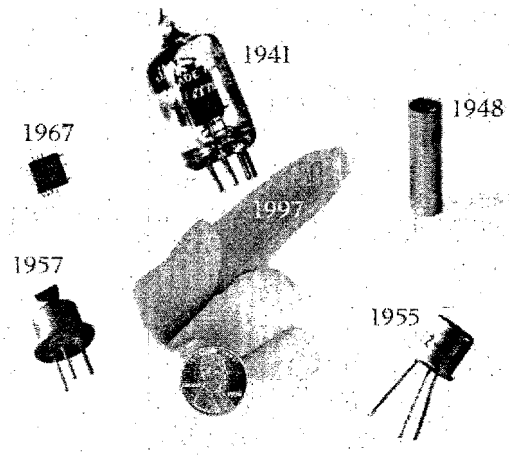


Figura 1.3.1-5 Transiciones del transistor

El procesador digital de señal es al los sistemas de radiocomunicación como lo es el microprocesador a la computadora. Un DSP contiene muchos circuitos individuales que hacen diferentes cosas. Un chip DSP apropiadamente equipado, puede comprimir señales digitales, así se reduce el ancho de banda requerido y/o se optimiza. Permitiendo mas canales de comunicación en la misma cantidad del escaso espectro de radio. Con un chip DSP simple, sistemas completos digitales celulares como GSM y TDMA pueden hacer sensitivamente económico. Dependiendo de diseño, al menos tres llamadas en un sistema digital pueden ocupar

el mismo canal o espacio de radio frecuencia de un canal simple análogo. Los chips DSP de ahora corren alrededor de 35 000 000 de instrucciones por segundo.

1997, los laboratorios Bell continúan con innovaciones. Modernas técnicas de fabricación facilitan poder empacar 5 millones de transistores en un simple chip y 200 chips en un obleas simple de ocho pulgadas cuadradas de silicio.

1.3.2 Radiocomunicaciones.

Los satélites también funcionan en base a enlaces de radio y no solo en épocas de guerra se utilizan para obtener información sobre cuestiones como espionajes, reconocimientos de instalaciones y posesión de armamento, investigación de la tierra y educación educativa a distancia entre otras.

Los enlaces de radio son el soporte de dos de las formas de transmisión de mayor éxito en la actualidad: las comunicaciones satelitales y la radiotelefonía móvil celular, que a su vez han evolucionado hacia las redes de comunicaciones personales, cuya base técnica primordial es la no-supeditación a redes de cable inmóviles.

Desde mi punto de vista y a pesar de que los sistemas de radiocomunicación tienen varias aplicación en esencia dependen de tecnologías comunes es por esto que los sistemas de comunicación por cables (telegrafía y luego telefonía), los sistemas de comunicación inalámbricos (radios de dos vías, enlaces punto-punto, radio aficionados, sistemas troncalizados, sistemas de telefonía celular, sistemas de comunicación satelital y ahora redes WLAN) dependen de tecnologías muy comunes y por lo que el avance de una hacer que cualquiera de las otras también avance. También, para el caso de los sistemas inalámbricos y dado que estas viajan por el espacio los efectos negativos y benéficos de este medio, los podemos encontrar en las redes WLAN.

Como vemos los sistemas inalámbricos empezaron principalmente para la transmisión de voz, pero últimamente se utilizan no solo para voz sino también para la transmisión de datos, en enlaces punto-punto y enlaces punto-multipunto,

permitiendo la comunicación entre dispositivos localizados remotamente sin la necesidad de un enlace por cable de por medio. El origen de las redes de área local (LAN) se centra principalmente en la interconexión de computadoras. Siendo

Estas redes, redes alambradas de una o de otra forma, con cable trenzado, cable coaxial e incluso cable de fibra óptica.

Como vemos la tendencia de las redes WLAN va a aumentar la velocidad de transmisión así como sus niveles de seguridad lo que las volverá cada vez mas confiables y de mayor uso en todos los niveles, publico o privado.

1.4 Fundamentos de telecomunicaciones

En la Figura 1.4.1-1 se muestran las unidades básicas comprendidas en un sistema de comunicación. No todos los sistemas incluyen la totalidad de las operaciones indicadas, aunque siempre emplean un medio de transmisión de alguna clase. El codificador elige la mejor forma de la señal para optimizar su detección en la salida. El decodificador efectúa la operación inversa para tomar la mejor decisión, basada en las señales disponibles, de que un mensaje dado fue efectivamente enviado. El diseño del codificador y el decodificador debe basarse en una detallada descripción matemática de la transmisión de información, un motivo más importante en muchos sistemas de comunicación modernos es mejorar la eficiencia en la conducción de la información.

El modulador produce una señal variable en la salida, que es proporcional, de algún modo, a la señal que aparece en sus terminales de entrada. Por ejemplo, un modulador senoidal puede variar la amplitud, la frecuencia o la fase de una señal senoidal en proporción directa a la tensión de entrada. Las funciones del codificador y del modulador son semejantes respecto a la preparación de la señal para una transmisión más eficiente. Sin embargo, el proceso de codificación está concebido para optimizar la detección de errores en un mensaje que se está transmitiendo, mientras que el proceso dé modulación está diseñado para imprimir la señal de

información sobre la onda que se va a transmitir. El demodulador realiza la operación inversa al modulador para restaurar la señal a su forma original.

Sin él medio de transmisión no existirían problemas de comunicación. El medio de comunicación puede incluir la ionosfera, la troposfera, el espacio libre o simplemente una línea de transmisión. En todo caso se introducen la atenuación y la distorsión, así como las señales de ruido generadas en los medios y en los equipos de transmisión y recepción. Las señales de ruido son cualesquiera señales eléctricas (tensiones o corrientes) que interfieran con la recepción libre de errores de la señal portadora del mensaje.

Las líneas verticales continuas de la Figura 1.4.1-1 indican tres subsistemas básicos de un sistema de comunicación. El subsistema central restringe el flujo de información y se llama canal. El canal incluye los efectos del ruido aditivo, la interferencia, la propagación y la distorsión. Es el factor limitante del rendimiento de cualquier sistema de comunicación bien diseñado. La función del transmisor es preparar la información para enviarla en forma tal que pueda superar lo mejor posible las limitaciones impuestas por el canal. La función del receptor es efectuar las operaciones inversas a las del transmisor para recuperar la información con la menor cantidad de errores posible. Nótese que, en sentido amplio, el transmisor y el receptor, en pareja, están diseñados de manera específica para combatir los efectos perniciosos del canal en la transmisión de información.

1.4.1 Simplex

El sistema de comunicación mostrado en la Figura 1.4.1-1 es capaz de transmitir en un sentido y se llama sistema de transmisión Símplex (SX). En muchos casos es deseable mantener una comunicación en dos sentidos o, al menos, poder devolver un mensaje a su origen para una posible verificación, comparación o control. Se transmite información únicamente en una dirección lo que significa que en cualquier momento, entre dos elementos de comunicación, solo uno transmite y por consiguiente el otro solo recibe.

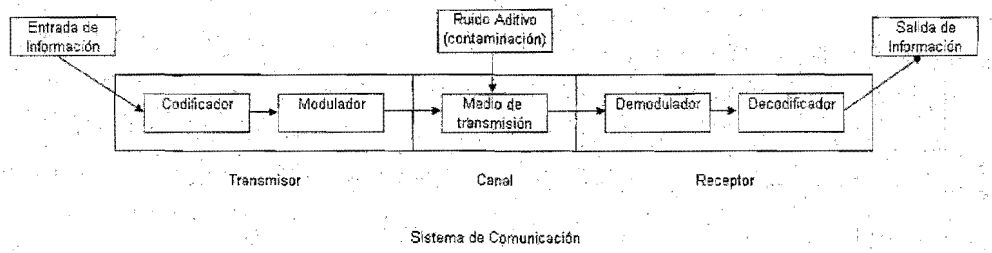


Figura 1.4.1-1 Sistema de comunicación

1.4.2 Half duplex

Este método se llama semi-dúplex (HDX, half-dúplex). Se transmite en ambas direcciones, pero solo en una dirección a la vez. Como ejemplo suponga la comunicación entre la terminal A y la terminal B, cuando la terminal A transmite y la terminal B solo recibe, cuando la terminal A termine de transmitir su información, entonces la terminal B puede iniciar su transmisión, si es así ahora la terminal A solo recibe. Una manera de obtener esto es utilizar el mismo canal de manera alterna para transmitir en ambas direcciones, como se muestra en la Figura 1.4.2-1, Sistema de comunicación Half-Duplex.

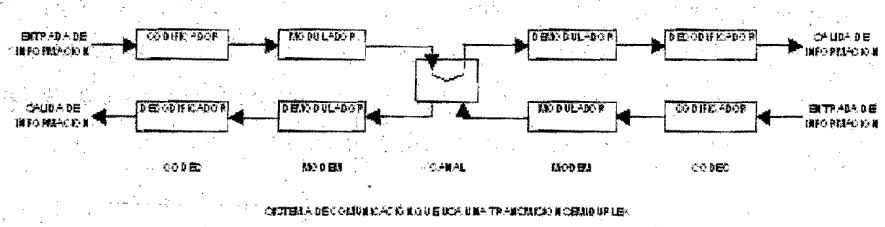


Figura 1.4.2-1 Sistema de comunicación Half-Duplex

Aunque la comunicación fluye en ambas direcciones, en un momento dado el flujo de información se realiza en un solo sentido.

1.4.3 Full duplex

En la Figura 1.4.3-1 se muestra un tercer tipo, el dúplex completo (FDX, Full-dúplex). En este, se obtiene comunicación simultánea en ambos sentidos. Nótese que tanto en la transmisión HDX como en la FDX, los moduladores y demoduladores operan en parejas. Esta combinación de modulador y demodulador se llama módem (modulador demodulador) en los sistemas de transmisión de datos.

También los codificadores y decodificadores trabajan en pares, dando así origen al término Codec (codificador decodificador). Se transmite simultáneamente en ambas direcciones. Esto es en cualquier momento, para dos terminales A y B, pueden estar recibiendo y transmitiendo al mismo tiempo si así lo requieren.

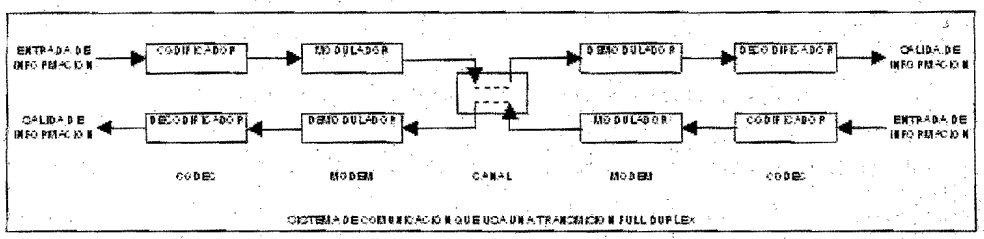


Figura 1.4.3-1 Sistema de comunicación full duplex

La transmisión en modo Simplex es común en televisión y radio comercial. No se usa habitualmente en comunicación de datos debido a la naturaleza unidireccional del proceso. Se utiliza no obstante, en algunas aplicaciones como telemetría.

La transmisión Semi-duplex se encuentra en muchos sistemas, como los sistemas de pregunta/respuesta, en los que un ETD envía una pregunta a otro ETD y espera a que el proceso de aplicación obtenga o calcule la respuesta y la envié de vuelta, otro ejemplo serian los radios de dos vías configurados de esta manera con la misma frecuencia en transmisión y recepción, lo que los obliga a usar un esquema Semi-duplex, solo uno transmite mientras todos los demás reciben.

El Full-duplex proporciona transmisión simultánea en dos sentidos, es ampliamente utilizado en aplicaciones que requieren un uso continuo del canal, alto rendimiento y tiempos de respuestas rápidos, como ejemplo tenemos los enlaces de microondas.

Considérese ahora un canal en el que el único perjuicio a la transmisión proviene del ruido aditivo. Como ya se mencionó, para la comunicación es necesario un ancho de banda mínimo B. Un ancho de banda mayor permitiría más interferencia del ruido

con la transmisión de información, por lo que es importante mantener el ancho de banda de dicho canal tan reducido como sea posible.

El ruido presente se caracteriza por su potencia media N y la señal transmitida por su potencia media S. Si la potencia media del ruido es relativamente pequeña, la potencia de la señal no necesita ser muy grande para que el receptor determine qué información se está enviando (por supuesto, también interesa la eficiencia y, por tanto, se intenta minimizar la potencia transmitida necesaria para conducir la información al usuario) Por el contrario, la potencia media de la señal debe ser relativamente grande cuando la potencia del ruido es grande. Así, se deduce que lo que importa es la razón entre la potencia media de la señal y la potencia media del ruido, y no las propias magnitudes de S y N. Esta razón S/N, llamada razón señal a ruido, es un importante parámetro en la teoría y el diseño de sistemas de comunicación.

Todos los sistemas de comunicación pueden juzgarse en términos de ancho de banda, razón señal a ruido y factores económicos (costo). Se supone (al menos de manera provisional) que los sistemas de comunicación son digitales y, especificamente, binarios. Supóngase, pues, que la información que se desea enviar en un momento dado puede caracterizarse por una muestra de entre n posibles entradas, todas con la misma probabilidad de ocurrencia. Por ejemplo, esta muestra podría ser uno de 256 niveles de tensión igualmente probable. Para enviar esta muestra usando un sistema binario, primero se genera una palabra digital compuesta por m símbolos binarios. Por tanto, cada palabra binaria consta de $m=\log_2 n$ dígitos binarios para representar una muestra de entre $n = 2^m$ posibilidades. Cuando se usa de esta manera, m se llama número de bits (binary digits, dígitos binarios) necesarios para representar a uno de entre n posibles estados de entrada. Por ejemplo, en este caso se necesita una palabra de ocho bits para describir uno de los 256 posibles estados de entrada.

A continuación, se desea enviar esta palabra binaria de m bits en sucesión a través del canal. En un sistema binario, estos bits se representan con símbolos binarios (p.

ej., + 1 y - 1) que se generan a razón de r símbolos por segundo. La tasa de información desde el transmisor es R = mr bits por segundo (bps) En el receptor, la señal transmitida se adultera por la adición de ruido y, como resultado, el receptor cometerá algunos errores. Se antoja razonable que la cantidad de errores disminuya si aumenta S/N. También parece razonable que puedan reducirse los errores con un receptor diseñado para procesar señales de mayor complejidad. Entonces, ya que el interés se centra tanto en la eficiencia como en la precisión de la comunicación, la siguiente es una pregunta de gran importancia: para un canal dado y para una tasa de transmisión de información dada, ¿es teóricamente posible mejorar el sistema con el objeto de reducir los errores?

$$C = B\log\left(1+\frac{S}{N}\right) \text{ bps}$$

Ecuación 1.4.3-1 Ley de Hartley Shannon

La respuesta, con base en el trabajo teórico de Claude Shannon publicada en 1949 es afirmativa si la tasa de transmisión de información es tal que R ≤ C, donde C es la capacidad del canal. Para el tipo de canal considerado aquí, la capacidad está dada por la ley de Hartley-Shannon.

Donde B es el ancho de banda del canal en (Hz.) y S/N es la razón señal a ruido. Si se intenta enviar información con demasiada rapidez es decir, R > C, los errores empiezan a aumentar aceleradamente y no tiene sentido tratar de diseñar un sistema para mejorar la situación. Por otra parte, si R < C, hay cierta esperanza de mejorar a través de un buen diseño del sistema.

Prosiguiendo con el razonamiento intuitivo, supóngase que se decide aumentar la tasa de transmisión de información aumentando la rapidez de los símbolos r. Puesto que son posibles más transiciones de símbolos por segundo, debe aumentarse el ancho de banda necesario. Por tanto, se puede lograr un aumento en la tasa de la información con un aumento del ancho de banda. Con esto simplemente se destaca

la conclusión que podría obtenerse de la aplicación directa de la Ecuación 1.4.3-1. Sin embargo, lo sorprendente es que la Ecuación 1.4.3-1 establece que el ancho de banda y la razón señal a ruido se pueden intercambiar. Por tanto, si se aumenta el ancho de banda, se puede lograr una razón S/N menor, y viceversa. Nótese que con S/N pequeño, el intercambio potencial es aproximadamente lineal,

Pero es exponencial para S/N grande. La ley de Hartley-Shannon es aplicable a sistemas tanto continuos como discretos, por lo que es un resultado de gran poder y alcance. No obstante, su aplicación se restringe a canales con ruido aditivo, y no se incluyen efectos como la distorsión y la interferencia.

$$\log_2(1+x) \approx ((\log_2 e)x \qquad \text{para x pequeña}$$

Ecuación 1.4.3-2

La de ley de Hartley-Shannon establece que existen cotas para la máxima tasa de transmisión de información en un canal dado y plantea que el ancho de banda puede intercambiarse con S/N, pero no ofrece un método para diseñar un sistema que cubra estos requisitos. En otras palabras, fija una cota con la que puede compararse el comportamiento de los sistemas que se diseñan, pero no da un procedimiento para diseñar sistemas cuyo comportamiento se ajuste a esa cota.

1.4.4 Estructura de una red de comunicaciones.

Habitualmente los programas de aplicación de empresas son ejecutados sobre sistemas de comunicación. El proceso de aplicación (PA) es la aplicación que maneja el usuario final. Habitualmente es un programa de computadora. Ejemplos pueden ser programas de contabilidad, de nominas, de reservas de boletos de avión, control de inventarios o una notebook.

El nodo A podría ejecutar un programa de aplicación (AP_{AI}) en forma de programa para acceder al proceso de aplicación en el nodo B (que es, en este caso, el programa [AP_{B1}] y una base de datos), hay también un programa en el nodo B

(AP_{B2}) que accede a un archivo en el nodo A mediante un programa de aplicación (AP_{A2}). Entiéndase proceso de aplicación para describir aplicaciones de usuario final, a menos que se indique lo contrario.)

La aplicación reside en el equipo terminal de datos, o ETD. ETD es un término genérico para designar a la máquina de usuario final, habitualmente una computadora o un terminal. Un ETD puede ser una gran computadora, como una estación de trabajo o un Servidor, o una PC de escritorio o notebook.

En la industria, un ETD puede tomar muy diversas formas. He aquí algunos ejemplos:

1. Una estación de trabajo para control de tráfico aéreo.
2. Un cajero automático de un banco.
3. Un terminal de punto de venta en unos almacenes.
4. Un dispositivo sensor para medir la pureza del aire.
5. Una computadora utilizada para automatizar el proceso de fabricación de una fábrica.
6. Un terminal o computadora con correo electrónico e Internet.
7. Una computadora personal en casa o en la oficina.

La finalidad de las redes de comunicaciones es conectar ETD de forma que puedan compartir recursos, intercambiar datos, apoyarse entre sí y permitir a los empleados realizar su trabajo desde lugares geográficamente remotos.

Una red proporciona comunicaciones lógicas y físicas entre las terminales y computadoras conectadas. Las aplicaciones y archivos emplean el canal físico para realizar comunicaciones lógicas. En este contexto, lógica significa que los ETD no necesitan saber nada de los aspectos físicos del proceso de la comunicación. La aplicación Al sólo necesita realizar una solicitud lógica de lectura con una identificación de los datos. A su vez, el sistema de comunicaciones es responsable de enviar la orden de lectura a través de los canales físicos a la aplicación B1.

También el equipo terminal del circuito de datos, o ETCD (también denominado equipo de comunicación de datos) Su función es conectar los ETD al canal o línea de comunicaciones. Los ETCD diseñados en los años 60 y 70 eran estrictamente dispositivos de comunicaciones. Sin embargo, en la última década los ETCD han incorporado muchas funciones de usuario, y hoy en día algunos contienen parte de los procesos de aplicación. No obstante, la función primordial de los ETCD sigue siendo servir de interfaz entre el ETD y la red de comunicaciones. El familiar módem es un ejemplo de ETCD.

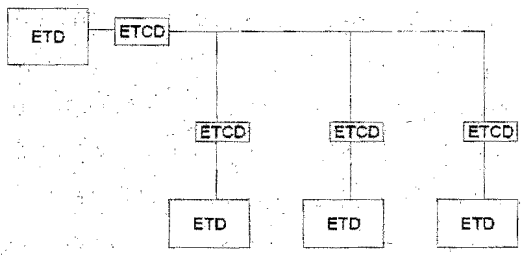


Figura 1.4.4-1 Circuitos Multipunto

Las interfaces se especifican y establecen mediante protocolos. Los protocolos establecen la forma en la que los ETD y la parte de comunicaciones intercambian información entre sí. Pueden incluir regulaciones, que estipulan una convención o técnica requerida o recomendada. Típicamente, para soportar una aplicación de usuario final se requieren varios niveles de interfaces y protocolos.

Hoy en día, muchas organizaciones están adaptando interfaces y protocolos comunes, como resultado de los esfuerzos a escala mundial para proporcionar estándares independientes de los vendedores y los productos.

1.4.5 Circuitos punto a punto y multipunto

Los ETD y los ETCD se pueden conectar de dos formas, se pueden conectar en una configuración punto a punto. En ella, sólo hay dos ETD conectados a la línea o canal. En la Figura 1.4.4-1 podemos ver otra configuración, denominada multipunto.

En esta configuración hay más de dos dispositivos conectados a un mismo canal. Los ETD y ETCD pueden intercambiar tráfico de comunicaciones en tres formas: simplex, half-duplex y full-duplex.

1.5 Introducción a las redes WLAN

Las redes inalámbricas, como muchas de las tecnologías vienen de aplicaciones militares. Donde las necesidades militares son las de disponer de una red simple, fácil y segura dentro de ambientes de combate.

Como los costos de redes inalámbricas se reducen y la calidad se incrementa se vuelve una relación costo-beneficio a favor de las empresas para integrar redes inalámbricas en sus empresas. Las tecnologías inalámbricas ofrecen una manera relativamente barata para conectar oficinas con otras oficinas sin la necesidad de cablear cables de cobre o de fibra óptica. Ahora el costo de las redes inalámbricas es tal que muchas empresas pueden implementar segmentos inalámbricos en sus redes ahorrando tiempo y dinero mientras que se mantiene la flexibilidad del Roaming. Los usuarios caseros también se ven beneficiados por los bajos costos y la subsiguiente disponibilidad de hardware de red inalámbrico.

1.5.1 Aplicaciones de redes inalámbricas.

Cuando las computadoras fueron construidas, solo las grandes universidades y corporaciones podían disponer de ellas. Ahora podemos encontrar incluso en casas con redes de dos o más computadoras dentro de nuestro vecindario (ejemplo los café Internet) Las redes inalámbricas están tomando el mismo camino, primero usadas por grandes empresas y ahora disponible para todos nosotros a un precio relativamente bajo.

Las LAN inalámbricas son frecuentemente implementadas como puntos de acceso, significando esto que ellos son utilizados como puntos de acceso para la conexión a una red alambrada. En el pasado el acceso estaba definido como un dial-up, ADLS, cable, celular, Ethernet, Token Ring, Frame Relay, ATM, etc. Los inalámbricos es

otra forma de acceso. Debido a la escasez de velocidad, las redes inalámbricas no son implementadas en el rol de distribución o núcleo de red. Por su puesto las pequeñas redes pueden no haber diferencia entre las capas de núcleo, distribución y acceso. La capa de núcleo de red debe ser muy rápida y estable, capaz de manejar cantidades grandes de tráfico con pocas dificultades y pocas probabilidades de salir de operación. La capa de distribución de la red, debe ser rápida, flexible y confiable. Las LAN inalámbricas no proporcionan del todo estos requerimientos para una solución empresarial.

Las redes inalámbricas ofrecen solución a un problema específico: movilidad. Las soluciones de telefonía móvil han estado disponibles por algún tiempo, ofreciendo a los usuarios la habilidad de vagar de un lado a otro mientras se mantienen conectados a baja velocidad y alto precio. Las redes LAN inalámbricas, ofrecen la misma flexibilidad sin las desventajas del alto precio y el alto costo, además de que pueden ser instalados en cualquier lugar.

1.5.2 Extensiones de red.

Las redes inalámbricas pueden funcionar como extensión de una red alambrada. Esto puede ser cuando se requiere extender la red alambrada y por consiguiente se requiere de instalar cables e infraestructura. Esto puede ser considerablemente caro si se considera todo lo que involucra, cableado de red, cableado eléctrico, canaletas, ductos, etc. Si además pudiera existir una distancia demasiado larga como para usar cable de categoría 5 (Cat5), entonces se deberá usar fibra óptica requiriendo incrementar en costo de la ampliación de la red, dado que además se requerirá de switch con conexiones para fibra óptica.

Las rede WLAN pueden fácilmente ser implementadas proporcionando conectividad a áreas remotas sin requerir de costos de implementación.

1.5.3 Conectividad edificio a edificio

En un ambiente de campus o en un ambiente con dos oficinas continuas donde se requierà conectar los edificios a la misma red, era necesario conectar los edificios ya sea instalando cables bajo tierra de una oficina a otra, o rentando una costosa línea dedicada de una oficina de telefonía local.

Usando tecnología de redes inalámbricas, los equipos pueden ser instalados fácil y rápidamente para permitir a dos o más oficinas ser parte de la misma red. Con las apropiadas antenas, cualquier número de oficinas pueden ser enlazadas a la misma red. Ciertamente hay límites para el uso de tecnología inalámbrica como los hay en cualquier solución de conectividad de datos, pero la flexibilidad, rapidez y el ahorro de costos de dinero y tiempo, hacen de las redes inalámbricas algo indispensables.

Hay dos tipos diferentes de conectividad de edificio a edificio la primera es llamada punto a punto (PTP) y la segunda es llamada punto a multi-punto (PTMP) Los enlaces PTP, son conexiones inalámbricas solo entre dos edificios, donde se usan antenas direccionales de alta ganancia. Los enlaces punto a multi-punto, son conexiones inalámbricas entre tres o más edificios, donde el edificio principal es usado como un concentrador de los demás edificios por lo que este usa una antena omnidireccional, mientras que los demás edificios usan antenas direccionales. Como se ve esta sería una implementación con topología de estrella.

1.5.4 Entrega de datos de última milla

Los proveedores de servicios de Internet inalámbrico (WISPs) ahora están tomando ventaja de los recientes avances en la tecnología inalámbrica para ofrecer la entrega de datos de última milla. "Ultima milla" se refiere a la infraestructura de comunicación (por cable o inalámbrica) que existe entre la oficina central de la compañía de telecomunicaciones y el usuario final.

1.5.5 Movilidad

Como una solución de capa acceso, las LAN inalámbricas no pueden remplazar a las LAN por cable en términos de velocidad (100basetx a 100 Mbps contra IEEE 802.11 A 54 Mbps) un ambiente inalámbrico usa conexiones intermitentes y tiene altas tasas de errores, como resultado las aplicaciones y protocolos de mensajes diseñados para redes alambradas algunas veces operan pobremente en un ambiente inalámbrico. Sin embargo las redes inalámbricas han creado la habilidad de transferir datos sin un excesivo uso de tiempo y recurso humanos para el ingreso de los datos de forma automática en una terminal móvil. Permitiendo a los usuarios moverse a lo largo de la cobertura de su red inalámbrica sin perder la conectividad a la red principal. Las capacidades del Roaming han incrementado la productividad de las organizaciones.

1.5.6 Pequeñas oficinas, oficinas en casa (SOHO)

Como profesionales de IT, podemos tener en casa más de una computadora. Estas computadoras podrían estar conectadas en red para poder compartir archivos, impresoras o conexiones de banda ancha.

Este tipo de configuración es también utilizado en pequeñas empresas con solo unos cuantos empleados. También estas empresas necesitan compartir para incrementar la productividad y la eficiencia.

Para estas aplicaciones en SOHO, las redes LAN inalámbricas son una solución muy simple y efectiva, sin la necesidad de implementar una red LAN por cable que requiera instalar cables y a su vez canalizar estos a través de muros y techos de la oficina.

1.5.7 Oficinas móviles

Las oficinas móviles permiten a muchas empresas implementar una red de computadoras en él sitió donde así lo requiera su trabajo, con equipo móvil como

computadoras portátiles, redes inalámbricas y un local portátil, muchas empresas pueden ofrecer sus servicios a donde un cliente a sí lo solicite, o llevar toda su oficina hacia una exposición donde requieran puntos de venta, bases de datos para los puntos de venta, impresoras para la facturación, conexión vía VPN para enviar su información sobre de los productos vendidos a la oficina central, monitores de computadora donde realicen una presentación de los productos ofrecidos por la empresa. Hay muchos grupos que requieren el uso de redes móviles, entre estos, organizadores de eventos deportivos, puntos de venta para espectáculos, circos, carnavales, exhibiciones, compañías de construcción, servicios de asistencia médica en casos de desastre, etc.

Debido a la saturación en algunas escuelas, estas están utilizando las redes inalámbricas para conectar sus salones provisionales al edificio principal, esto mientras se construyen nuevos salones.

1.6 Situación Actual en México.

Las comunicaciones inalámbricas en México, están tomando fuerza en los últimos años, las redes inalámbricas, por ejemplo, las redes inalámbricas celulares con estándares como AMPS (Advanced Mobile Phone System), sistema analógico donde su principal aplicación es la voz, IS-95 (CDMA) estándar de telefonía móvil digital utilizando tecnología CDMA (Acceso Múltiple por División de Código), maneja voz y datos en proporción menor, IS-136 (TDMA) estándar digital que utiliza TDMA (Acceso Múltiple por División de Tiempo), maneja voz y datos en menor proporción, GSM (Sistema de Telefonía Móvil Global), este estándar tiene varias versiones y constantemente lo están actualizando, por lo que el estándar que conocemos en México es una versión mejorada de la versión inicial, esta versión maneja voz y datos, pero en la sección de datos tuvo una mejora por lo que este incluye entre otras la tecnología GPRS (Sistema de radio paquetes general) lo cual hace más versátil la transmisión de datos. Este sector de telefonía móvil tiene varias propuestas unificadas en varios estándares pero definidas como telefonía de tercera generación que incluye mejorar en la comunicación de datos principalmente.

Por otro parte y paralela a la telefonía celular están las redes inalámbricas (WLAN) cuyo estándar principal el 802.11, de esta se derivan las siguientes:

802.11a

802.11b

802.11g

Estas son tecnologías de acceso de la capa 1 y 2 del modelo OSI y permiten interconectar redes inalámbricas a redes alambradas, manejando varias velocidades y frecuencias de acceso, aunque por el momento se habla de nuevos estándares por venir que implementan ciertas mejoras con respecto a las anteriormente citadas, como son:

802.11e	estándar para la calidad de servicio en redes WLAN
802.11i	estándar para reforzar la seguridad en redes WLAN
802.11n	estándar que incrementa la velocidad de transmisión
WiMax (802.16)	estándar para redes inalámbricas de largo alcance (WAN)

Ambas redes con la configuración adecuada nos permitirían conectar a la red y a Internet, pero las redes WLAN serian las más económicas dado que no dependen de una tarifa para su uso.

Las redes inalámbricas se están utilizando ampliamente en redes privadas y redes publicas, como sustituto de una red alambrada, como un servicio complementario a una red alambrada existente, como punto de acceso para proporcionar Internet de forma gratis (HotSpot), se habla incluso de utilizar al WLAN para interconectar teléfonos inalámbricos lo que trae como consecuencia un VoWLAN (Voz sobre Redes Inalámbricas)

Un punto importante a ser considerado y el cual todas las empresas quieren mejorar y/o fortalecer, es la seguridad, dado que nadie quiere que personas no autorizadas tengan acceso a la red, a los archivos de la empresa y/o a los servicios de la empresa.

Existen diferentes formas de implementar seguridad en las redes inalámbricas y todo depende de la complejidad que estemos dispuestos a implementar.

A pesar de que se discute ampliamente el tema de seguridad, las redes inalámbricas se han incrementado y según indicativos del mercado seguirá creciendo.

Las comunicaciones inalámbricas desde su creación e implantación han definido una nueva forma de comunicación en la sociedad cambian de manera radical la forma en como la gente realiza sus actividades que a diario realiza, las redes inalámbricas permiten al usuario final movilidad, algo que nunca antes era posible porque estábamos sujetos a las redes alambradas.

Con la llegada de las WLAN esto va cambiando paulatinamente, las WLAN permiten movilidad dentro de un área definida por el diseño de la WLAN.

Al interconectarnos a una red alambrada por medio de un Access Point, podemos disponer de los mismos servicios que ofrece una red alambrada como son:

Acceso a impresoras compartidas

Acceso a bases de datos

Internet

Servicios de Correo

Servicios de mensajeria

Acceso a computadoras compartidas

Videoconferencia.

Las primeras redes de computadoras estaban implementadas e interconectadas por cable trenzado o coaxial, actualmente predominan ampliamente las redes basadas en UTP, STP y fibra óptica. Pero más aun el medio inalámbrico esta tomando terreno en el campo de las redes de computadoras. Cuando las redes WLAN se presentaron en el mercado con dispositivos eran considerablemente caros, pero a medida que han surgido nuevos estándares, y se ha incrementado su demanda, los precios de estos dispositivos se han reducido ampliamente lo cual permite implantar una red sin la necesidad de gastar dinero e invertir tiempo para alambrar las instalaciones de una empresa.

Hoy en día, en México disponemos de algunos puntos de acceso en algunos restaurantes, aeropuertos, tiendas, incluso en algunas universidades privadas. Las redes inalámbricas permiten un acceso básicamente a Internet algunos puntos de acceso son gratis y algunos muy probablemente estén cobrando una cuota mensual relativamente baja.

La tendencia es hacia el incremento de las redes inalámbricas ya sea para uso publico o para uso privado, soportando una amplia variedad de aplicaciones, uno de los factores que favorecen a las redes WLAN es su rápida implantación sin la necesidad de realizar una planeación para tendidos de cableado estructurado, mas sus requerimientos son distintos y deben de tomarse en consideración para su instalación, como son, estudios de cobertura, implementación de medidas de seguridad, autenticación y encriptación de datos, etc.

1.7 Situación actual en la ENEP Aragón

Actualmente en la ENEP Aragón no existe una red inalámbrica, que permita a los estudiantes tener acceso a Internet sin la necesidad de hacer uso de algunas de las salas de computo existentes, para disponer de la información los estudiantes necesitan ir físicamente a alguna de estas salas de computo, perdiendo la capacidad de poder mezclar y comparar dos o mas fuentes de información en un mismo lugar

al mismo tiempo, por ejemplo investigar un tema de física en la librería al mismo tiempo bajar algún documento proveniente de Internet que le permitan a los estudiantes hacer una comparación y apreciación de la información que ellos investigan. La ENEP Aragón cuenta con varios centros de cómputo, que se han agregado paulatinamente desde el año de 1993 en que solo contábamos con un centro de computo instalado en el edificio para este fin, cerca del edificio del CELE y del edificio A-1, actualmente hay varias salas de computo instaladas en varios edificios como son:

3 salones de cómputo en la biblioteca

1 centro de cómputo en el edificio edificio A-5

1 centro de cómputo en el edificio A-4

Si analizamos esto veremos que el uso de la computadora se ha extendido incluso a carreras que no están directamente relacionadas con la computadora, pero que la utilizan como un medio de apoyo en el estudio de cualquier carrera en particular. Dado que se hace un uso intenso de las computadoras y de los servicios relacionados con estas (correo electrónico, Internet, Chat, procesadores de texto, etc.), incluso se esta usando a las computadoras como un apoyo para el aprendizaje de lenguas extranjeras, por lo que la demanda de estos servicios tendera a crecer. Una opción para poder extender la oferta de estos servicios, es permitir a los estudiantes la facilidad para conectarse a la red mediante dispositivos inalámbricos. Obviamente, la escuela sería la responsable de instalar, administrar y mantener la red inalámbrica de acuerdo a las políticas que mas convengan a esta, y los equipos móviles (computadoras, DPA y tarjetas de red inalámbricas) correría por cuenta de los estudiantes, si hiciéramos un comparativo entre el costo de instalar una sala de computo con todo el equipo de red y el equipo de computo, contra una red inalámbrica donde solo se requiere instalar equipos de red como puntos de acceso, router o switch y donde los equipos de computo correrían por cuanta de los usuarios veríamos que es mucho mas rentable una red inalámbrica, lo cual permitiría reducir

los costos de la instalación de nuevas salas. Para poder tener control del uso adecuado de la red inalámbrica se instalarían dispositivos en hardware y/o software para mejorar la seguridad y administración de la red.

La red inalámbrica permitiría extender los servicios de computo hacia regiones de la escuela hasta ahora no cubiertos como son: salones, explanadas, laboratorios, auditorios, además de que permitiría hacer uso de estos servicios a cualquier ahora sin depender de un horario de servicio.

Ofrecería la oportunidad de brindar más recursos para la enseñanza y aprendizaje tanto en clases en curso como fuera de estas.

1.8 Efectos en el sector estudiantil de la ENEP Aragón

La WLAN brida los mismos beneficios de una red alambrada para la comunicación de datos y constantemente mejora sus características para la transmisión de datos, la propuesta sugiere el uso del estándar recién aprobado en el año de 2003, y este es el 802.11g a 54 Mbps en la banda de 2.4 GHz.

Las redes inalámbricas proporcionarían más recursos a los estudiantes para que estos incrementen la calidad y cantidad de sus horarios de estudio sin importar en que parte de la escuela se encuentren, esta versatilidad solo es posible con las redes WLAN, (sin horarios y sin sitios fijos donde estudiar), todo esto permitiría incrementar la productividad de los estudiantes y al no depender de equipo de computadoras de los centros de computo de la escuela, permitiría ofrecer el servicio a un numero mayor de estudiantes.

A medida que se incremente la cobertura de la red WLAN, se podrá incrementar él número usuarios y de servicios así como la calidad de estos, creando en general un mejor ambiente para estudiar donde los miembros de la escuela tanto maestros como alumnos, y por que no hasta los trabajadores dispondrían de mejores elementos de comunicación.

Capitulo 2 Fundamentos teóricos de radiofrecuencia

2.1 Fundamentos teóricos radio frecuencia

Radio frecuencia es una señal de corriente alternada a alta frecuencia que es pasada a través de una conductor de cobre y después es radiada con una antena sobre el espacio libre. Una antena convierte/transforma una señal alambrada en una señal inalámbrica y viceversa cuando la señal de alta frecuencia es radiada en el aire, esta forman ondas de radio. Estas ondas de radio se propagan desde la fuente (la antena transmisora) en línea recta en la dirección del patrón de radicación de la antena.

2.1.1 Propagación radioeléctrica.

Todos los dispositivos de radio utilizan el espectro electromagnético para enviar información sobre el espacio (el aire en el planeta tierra) y estas ondas presentan ciertas características propias de estas, por lo que es importante entender como trabajan y son afectadas por el medio (el espacio libre.

Existen diferentes formas en como viaja una señal de electromagnética desde un punto transmisor a un punto receptor, cada una tiene sus características propias.

2.1.2 Línea de vista

La propagación por línea de vista es la cual se presenta cuando la señal viaja en forma directa de una antena a otra en forma directa, esto es, entre ambas antenas hay línea de vista y desde cualquiera de ellas es visible la antena del otro extremo, sin ningún obstáculo de por medio.

A menos que este muy cerca de tu antena destino, necesitaras mantener la antena lo mas alto posible. Debido a que las ondas de radio siguen una línea recta de esta manera, ellas simplemente van en el espacio siguiendo la curvatura de la tierra causado por la tierra.

Cuando elevamos la antena, la distancia hacia el horizonte se incrementa. Con suficiente potencia para alcanzar la otra antena y altura suficiente para verle, podemos hablar mantener el enlace de radio sin ningún problema. Los repetidores de VHF usualmente son montados en construcciones altas o en lo alto de las montañas por estas razones.

2.1.3 Propagación por ondas de tierra

La propagación de ondas de tierra no es una variación de la propagación por línea de vista de hecho, las ondas de tierra viajaran de forma adicional debido a la curvatura de la tierra empuja la señal hacia abajo manteniéndolas a lo largo de la tierra. Podemos alcanzar una antena la cual se encuentra por abajo del horizonte con propagación de ondas de tierra, pero desde que la señal interactúa con la tierra, pierde mucha energía a lo largo de su viaje hacia el destino limitando su rango.

2.1.4 Propagación por ondas espaciales

En este modo la señal es enviada hacia la ionosfera, 30 o 250 millas arriba de la superficie de la tierra. Dependiendo de cómo es la ionización y de la frecuencia que sé esta usando. Puede actual mas o menos como un espejo, reflejando la señal hacia abajo ha cierta distancia. Literalmente puede saltar sobre una amplia sección de un estado y regresar hacia abajo muchos kilómetros adelante.

2.1.5 Propagación de Radio

La calida de la transmisión de una onda electromagnética en línea de vista, depende mucho de los desvanecimientos que son causados por las variaciones de las condiciones de propagación de las ondas electromagnéticas o por efectos adversos atmosféricos o lluvia o el terreno.

Los desvanecimientos que ocurren así, son complicados, estos son generalmente discutidos en términos de varias categorías basadas en modo de las variaciones de la potencia recibida o basadas en la causa del desvanecimiento.

2.1.6 Desvanecimientos por absorción

Este desvanecimiento es la atenuación de la onda de radio causada por la absorción o dispersión debido a la lluvia, nieve, niebla, moléculas de gas en la trayectoria de propagación, estos afectan ampliamente a los rangos de frecuencia por encima de los 10 GHz.

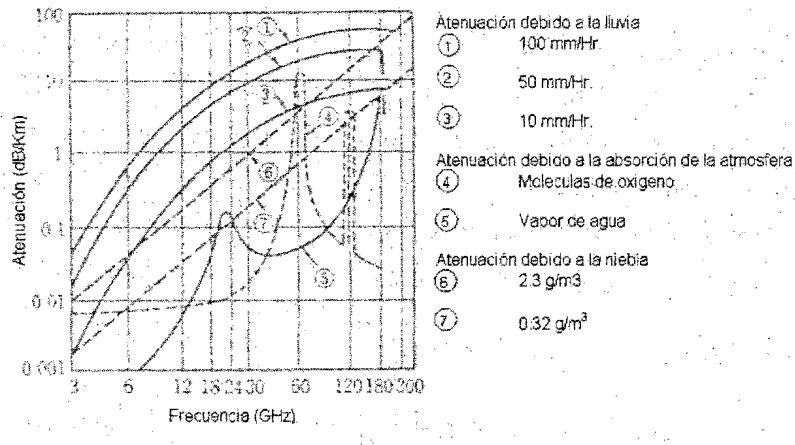


Figura 2.1.6-1 Desvanecimiento por absorción

2.1.7 Desvanecimientos debidos a obstáculos

Como se muestra en la Figura 2.1.7-1, la potencia recibida sometida a decrecimiento por interrupción en la ruta del rayo de la onda como resultado del obstáculo causado por la variación de K.

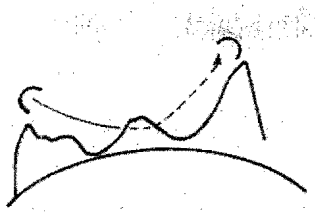


Figura 2.1.7-1 Desvanecimiento debido a obstáculo

2.1.8 Desvanecimientos debidos a ductos

Cuando hay un fenómeno de ducto, aparece una zona ciega la cual previene que las ondas de radio sean recibidas.

Cuando el efecto ductos es muy fuerte, la atenuación se incrementa, la potencia recibida decrece por abajo del nivel de umbral, y la transmisión de la señal es interrumpida por algún tiempo.

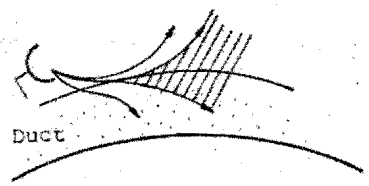


Figura 2.1.8-1 Desvanecimiento debido a efecto ducto

Las ondas que pasan a través del ducto son sujetas a los efectos divergencia y convergencia del ducto, y la potencia recibida muestra diferentes valores a los del espacio libre. Especialmente cuando los efectos de la convergencia aparecen, la potencia recibida se incrementa (esto es llamado up-fading) y en algunos casos es 10 a 20 dB arriba del cálculo de espacio libre.

2.1.9 Desvanecimientos por interferencia

Los desvanecimientos por interferencia, también llamados desvanecimientos por multi-trayectoria, ocurren como sigue:

Cuando dos o más rayos con diferente longitud de trayectoria son recibidos debido a la reflexión o refracción como se muestra en la Figura 2.1.9-1, la fuerza del campo, las características amplitud vs. Frecuencia y las características de retardo vs. Frecuencia de la señal combinada varía con la amplitud y diferencias de fase entre los rayos recibidos.

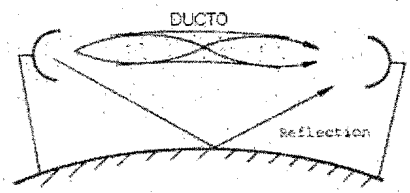


Figura 2.1.9-1 Desvanecimiento debido a interferencia

2.1.10 Reflexión.

La reflexión ocurre cuando una onda electromagnética es afectada por un objeto que es de dimensiones muy grande con relación a la longitud de onda de la señal electromagnética. La reflexión ocurre en la superficie de la tierra, construcciones, muros y muchos otros obstáculos. Si la superficie es lisa, la señal reflejada puede causar serios problemas a las redes LAN inalámbricas. Estas señales reflejas en objetos, son referidas como señales multi-trayectoria (multi-path) Las multi-trayectoria pueden causar efectos adversos en las redes WLAN, tales como degradación o cancelación de la señal principal y causar agujeros o vacíos en área de cobertura de la señal de RF. Superficies como lagos, techos de metal, puertas de metal y otros pueden causar reflexiones severas y por lo tanto señales de multi-trayectorias.

2.1.11 Refracción

La refracción se describe como la desviación de la onda de radio de su trayectoria original cuando esta pasa a través de un medio de distinta densidad al medio por donde viajaba originalmente. Cuando una señal pasa a través de otro medio, alguna parte de la señal será reflejada y otra parte de la señal pasara a través del medio y se doblara en otra dirección, dentro del nuevo medio. La refracción puede ser un problema muy serio para enlaces de larga distancia. Como las condiciones atmosféricas cambian, en índice de refracción puede cambiar a lo largo de la trayectoria y este puede provocar de la señal de radio cambie de dirección, desviándola de su destino original.

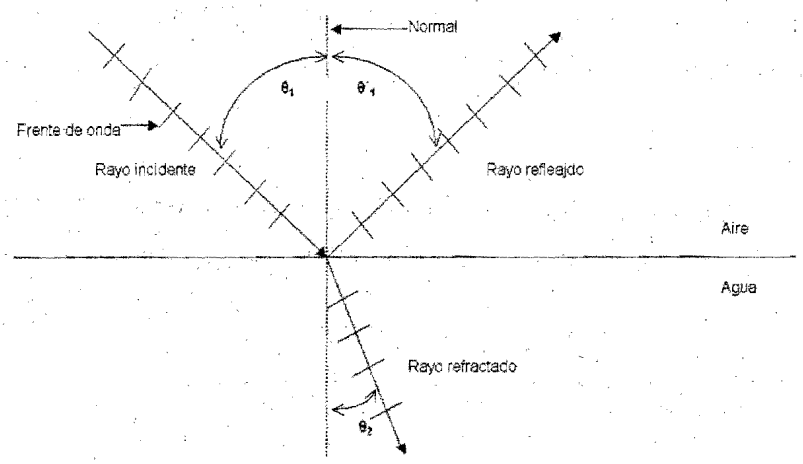


Figura 2.1.11-1 Reflexión y refracción

En la Figura 2.1.11-1 se muestra un haz que incide sobre la superficie plana de un medio distinto al aire (agua de un lago, por ejemplo) el haz de la señal se refleja de la superficie y se dobla (refracta) al entrar al agua.

El haz incidente queda representado por una línea recta, que es el rayo incidente, paralela a la dirección de propagación. Se supone que el haz incidente, es una onda plana cuyos frentes de onda son perpendiculares al rayo incidente. Los haces

reflejados y refractados también son representados por rayos. Los ángulos de incidencia (θ1), de reflexión (θ´1) y de refracción (θ2) se miden entre la normal a la superficie y el rayo correspondiente, tal como se muestra en la Figura 2.1.11-1. Las leyes que gobiernan a la reflexión y a la refracción son:

Los rayos reflejado y refractado se encuentran en el plano formado por el rayo incidente y la normal a la superficie en el punto de incidencia.

En la reflexión: $(\theta 1) = (\theta' 1)$

En la refracción $\text{sen}(\theta 1)/\text{sen}(\theta 2) = n_{21}$

En donde n_{21} es una constante llamada índice de refracción del medio 2 con respecto al medio 1. El índice de refracción de un medio respecto a otro generalmente varía con la longitud de onda.

2.1.12 Difracción

La difracción ocurre cuando la trayectoria de una señal de radio entre el transmisor y el receptor es obstruida por una superficie que tiene irregularidades filosas o de otra

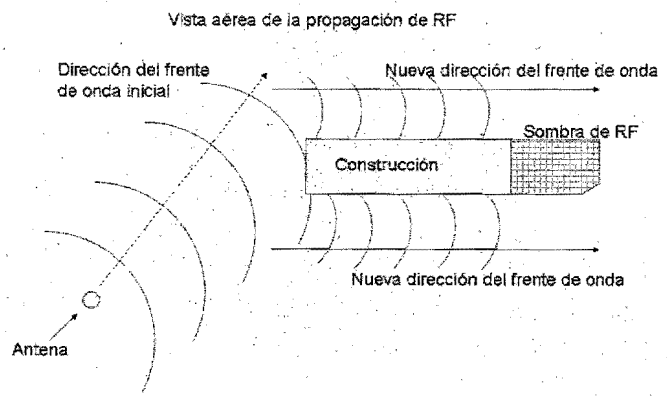


Figura 2.1.12-1 Difracción de RF

manera una superficie áspera. A lata frecuencia, como la reflexión, depende de la geometría de del objeto que obstruye la trayectoria de la onda en propagación y de la amplitud, fase, y polarización de la onda incidente en el punto de difracción. La difracción describe una onda doblada alrededor de un objeto.

2.1.13 Dispersión

La dispersión ocurre cuando un medio a través del cual las ondas viajan, consiste de objetos con dimensión que son pequeñas comparadas con la longitud de onda de la señal y el numero de obstáculos por unidad de volumen es grade. La dispersión de ondas es producida por superficies rugosas, objetos pequeños o por otras irregularidades en la trayectoria de la señal.

La dispersión puede ocurrir primero, cuando las ondas golpeen una superficie irregular es esta es reflejada en muchas direcciones simultáneamente. La dispersión de este tipo produce muchas reflexiones de pequeña amplitud y destruir la señal de RF principal.

Una segunda dispersión puede ocurrir cuando una señal viaja a través de partículas suspendidas en el medio, tales como polvo pesado. En este caso, las ondas de RF son individualmente reflejadas en muy pequeña escala en partículas pequeñas.

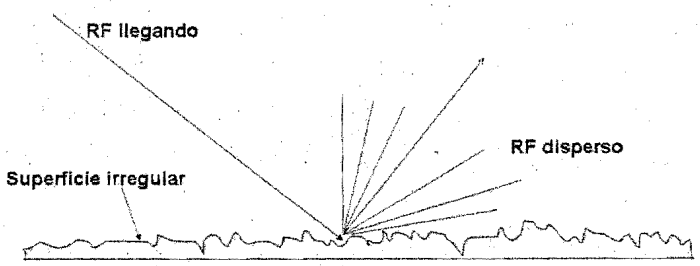


Figura 2.1.13-1 Dispersión de RF

2.1.14 Ganancia

La ganancia es él termino usado para describir un incremento en la amplitud de la señal de RF. La ganancia es usualmente un proceso activo, significando esto que una fuente de energía externa, tales como amplificadores de RF, son usados para amplificar la señal o antenas de alta ganancia son usadas para concentrar el ancho del rayo de la señal para incrementar la amplitud de la señal.

Sin embargo procesos pasivos pueden también causar ganancia. Por ejemplo señales de RF reflejadas pueden combinarse con la señal principal para incrementar la señal principal.

2.1.15 Perdidas.

Las perdidas describen una disminución en la amplitud de la señal. Muchas causas pueden provocar pérdidas de la señal de RF. Esto aplica tanto cuando la señal todavía esta en el cable en forma de señal eléctrica AC de alta frecuencia, como cuando es propagada como forma de ondas a través de del aire. La resistencia del cable y conectores causa perdida debido a la conversión de la señal eléctrica en calor. La diferencia de impedancia en los cables y conectores puede causar reflejos de potencia hacia la fuente de la señal, los cuales pueden causar degradación de la señal. Objetos ubicados directamente en la ruta de propagación de la señal, pueden absorber, reflejar o destruir la señal de RF. Las perdidas también pueden sé insertadas intencionalmente, directamente en el circuito con atenuadores de RF. Los atenuadores de RF son resistencias exactas que convierte la señal AC de alta frecuencia en calor para reducir la amplitud de la señal en el punto del circuito donde es instalado.

Es ser capaz de medir y compensar las perdidas en un circuito, es importante debido a que los receptores de los radios tienen un umbral de sensitividad. El umbral de sensitividad es definido como el punto en el cual el radio puede distinguir claramente una señal del ruido de fondo. Debido a que la sensitividad del radio es finita, la

estación transmisora debe transmitir una señal con la suficiente amplitud para ser reconocida en el receptor. Si ocurren perdidas entre el transmisor y el receptor es necesario remover el objeto que cause la perdida o incrementando la potencia del transmisor.

2.1.16 VSWR

El VSWR ocurre cuando las impedancias entre los dispositivos en un sistema de RF son distintas entre ellas, esto significa que una pieza del equipo tiene una impedancia mayor o menor a la impedancia del equipo a la cual se va a conectar. El VSWR es causado por la señal de RF reflejada en el punto donde el acoplamiento de impedancia es distinto en la trayectoria de la señal. El VSWR causa perdida por retorno, que es definido como la perdida de la energía enviada a través del sistema debido a alguna de la potencia reflejada hacia el transmisor. Si la impedancia de la terminación de la conexión no es igual a la impedancia del sistema, entonces la máxima cantidad de potencia transmitida puede no ser recibida en la antena. VSWR es una relación, que es expresada como la relación entre dos números. Valores típicos de VSWR podrían ser 1.5 : 1, El segundo número siempre es 1, y representa el perfecto acoplamiento de impedancias, mientras que el primero representa la variación de la impedancia con respecto al sistema.

Excesivo VSWR puede causar serios problemas en los circuitos de RF, la mayoría de las veces, el resultado es un descenso en la amplitud de la señal de RF transmitida. Sin embargo si los transmisores no están protegidos contra la potencia aplicada al transmisor (o retornada), la potencia reflejada puede quemar la electrónica del transmisor. Los efectos del VSWR son evidentes cuando el transmisor esta dañado, la salida de potencia es inestable, y la potencia observada es significativamente diferente de la potencia esperada. Lo métodos para cambiar el VSWR en un circuito incluyen el uso apropiado del equipo, conexiones entre cables y conectores, el uso de hardware para el acoplamiento de impedancia y el uso de equipo de alta calidad.

Para equipo de radio existen conectores y cables con impedancias de 50 ohms y 75 ohms por lo que se recomienda utilizar el adecuado para cada sistema a fin de evitar los efectos negativos del VSWR.

2.1.17 Principios de antenas

Algunos puntos para entender las redes LAN inalámbricas son la línea de la señal, los efectos de la zona de Fresnel y la ganancia de la antena.

Línea de la señal (LOS, Line of Sight)

Con una línea visual (LOS) es definida como la línea directa aparente desde un objeto que esta transmitiendo hasta el observador en un sitio de recepción. La LOS es aparente porque las ondas de luz están sujetas a cambios en la dirección debidos a la refracción, reflexión y difracción en la misma forma que las ondas de radio frecuencia. Las ondas de RF trabajan en la misma forma que las ondas de luz con la excepción de que la LOS de RF puede ser también afectada por bloqueos de la zona de fresnel.

2.1.18 Zona de Fresnel

Una consideración cuando se planea un enlace de RF, es la zona de fresnel. La zona de fresnel es importante para la integridad del enlace de RF debido a que define una área alrededor del "LOS" que puede interferencia de la señal de RF si es bloqueada. Objetos en la zona de fresnel tales como árboles, postes y construcciones pueden difractar o reflejar la señal principal enviada hacia el receptor cambiando la "LOS" de la RF. Los mismos objetos pueden absorber o dispersar la señal de RF principal causando degradación o pérdida de la señal completa.

El radio de la zona de fresnel en un punto puede ser calculado por la siguiente formula:

$$r = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

Ecuación 2.1.18-1 Radio de la zona de Fresnel

Donde: d1 y d2 distancias a punto del radio de fresnel

λ = longitud de onda de la señal en metros

r = es el radio de la zona de Fresnel

K es una constante =1 para la primer zona de Fresnel

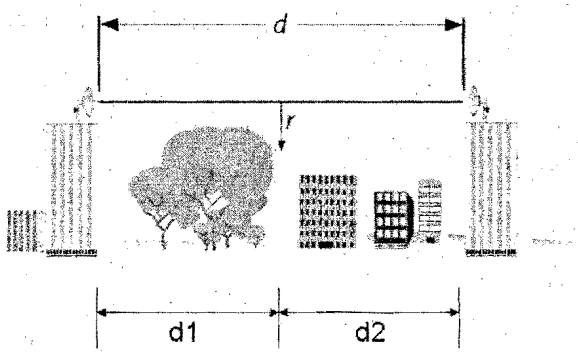


Figura 2.1.18-1 Radio de Fresnel

Considerando la importancia de la zona de fresnel, es importante cuantificar el grado en el cual la zona de fresnel puede ser bloqueada. Típicamente de 20 % a 40 % de bloque de la zona de fresnel introduce algo de interferencia en el enlace, es recomendable no exceder de 20 % en el bloqueo de la zona de fresnel. Obviamente una señal sin obstrucción seria el caso ideal. La forma de disminuir el bloqueo en la

zona de fresnel es elevar las antenas en un extremo o en ambos extremos para así elevar la LOS y su correspondiente radio de la zona de fresnel.

2.1.19 Ganancia de antena

Un elemento de antena sin amplificadores y filtros típicamente asociados a el, es un dispositivo pasivo. La antena puede crear el efecto de amplificación por virtud de su forma física. La amplificación de la antena es el resultado del enfoque de la radiación de RF en un fuerte haz, similar al rayo de luz de una lámpara, concentrado, creando un haz sumamente brilloso. El enfoque de la radiación es medida por medio de el ancho del haz, el cuales medida en grados horizontales y verticales.

2.1.20 Potencia radiada isotropica equivalente (EIRP)

EIRP es la potencia radiada por el elemento de antena y toma en cuanta la ganancia de la antena. Es la potencia que realmente sale de la antena y a la cual ya se incluyo también las perdidas de los elementos entre el transmisor y la antena.

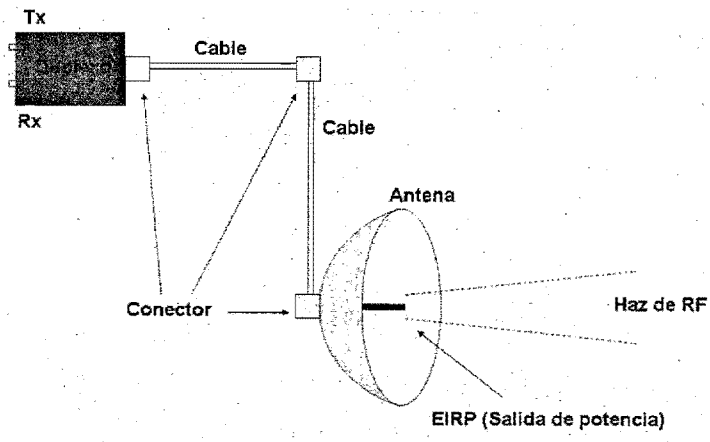


Figura 2.1.20-1 EIRP

Hay cuatro importantes áreas para el cálculo de potencia en una red inalámbrica y estas son:

8. La potencia del dispositivo que transmite.
9. Perdidas de dispositivos de conectividad
10. Ganancias de dispositivos de conectividad
11. Potencia antes y después de la antena

Los dispositivos de inter-conectividad pueden ser conectores, duplexores, divisores, cables, amplificadores, atenuadores, cavidades resonantes, aisladores, etc.

Cada uno de estos puntos debe ser considerado para el diseño y resolución de problemas de una red inalámbrica.

2.1.21 Unidades de medición

Son pocas las unidades de medición estándar utilizados en los equipos de radio como las WLAN, pero deben ser conocidos para poder entender y resolver problemas en las redes WLAN

2.1.22 Watts (W)

La unidad básica de la potencia es el Watt, y esta definido como la potencia utilizada por un elemento que por el circula una corriente de 1 ampere, teniendo este elemento entre sus extremos un voltaje de 1 Volt.

2.1.23 Miliwatt

Cuando se implementa redes inalámbricas, niveles de potencias tan pequeños como 1 miliwatt (1/1000 watt abreviado como mW), pueden ser usados para área pequeñas. Los dispositivos WLAN manejan potencias de entre 30 y 100 mW.

2.1.24 Decibel

Cuando un receptor es muy sensitivo a la señales de RF, puede detectar señales tan pequeñas como 0.000000001 watts. Los decibeles nos permiten representar estos números, haciéndolos mas manejables y entendibles. Los decibeles están basados en una relación logarítmica del valor de potencia expresado en watt.

La siguiente es la formula para convertir mW a dBm:

$$P_{dBm} = 10\log\left(\frac{Potencia(Watts)}{1mW}\right)$$

Ecuación 2.1.24-1 Relación dBm a Watts

Donde:

P_{dBm} = es la potencia expresada en dbm

Potencia en watt = es la potencia expresada en watt que queremos convertir a dBm

1 mW = es una referencia que nos sirve para referir los watt a miliwatt.

La ganancia y la perdida de potencia son medidas en decibeles no es watts debido a que las perdidas y ganancias son conceptos relativos y los decibeles son una medida relativa.

2.2 Espectro disperso

Espectro disperso es un técnica de comunicación caracterizada por el amplio ancho de banda y por su potencia pico baja. Las comunicaciones de espectro disperso usan varias técnicas de modulación en redes inalámbricas WLAN y poseen varias ventajas sobre su precursor, las comunicaciones de banda estrecha. Las señales de espectro disperso son como el ruido, difícil de detectar y también difícil de interceptar o remodular sin el equipo apropiado. Obstrucciones e interferencias tienen menos

efectos en una comunicación de espectro disperso en comparación a la comunicación de banda estrecha. Por esta razón, el espectro disperso ha sido ampliamente utilizado por los militares.

2.2.1 Transmisión de banda estrecha

La transmisión de banda estrecha es una tecnología de comunicación que usa solo el espectro de frecuencia suficiente para transportar la señal de datos y no más. El espectro disperso es la parte contraria a la banda estrecha, la señal de datos se dispersa en un ancho de banda que es mucho más amplio que el requerido para enviar la información.

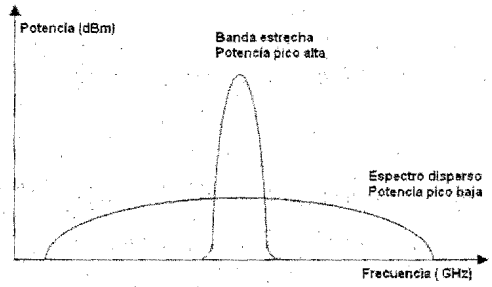


Figura 2.2.1-1 Banda estrecha vs. Espectro disperso en el dominio de la frecuencia

En la Figura 2.2.1-1, se ilustra la diferencia entre banda estrecha y espectro disperso, la banda estrecha requiere mas potencia para enviar datos cuando transmite usando un rango de frecuencia pequeño. Para que una señal de banda estrecha pueda ser recibida, esta debe de estar por arriba del nivel de ruido, llamado el piso de ruido, en una cantidad significativa. El pico alto de potencia asegura una recepción libre de errores en una señal de banda estrecha. Un argumento en contra de la banda estrecha es que puede experimentar interferencia o obstrucciones muy fácilmente debido a señales no deseadas en la misma banda como son otras señales de banda estrecha y ruido pueden eliminar completamente la información a través de traslapar la transmisión de banda estrecha.

2.2.2 Tecnologías de espectro disperso

Las tecnologías de espectro disperso nos permiten tomar la misma cantidad de información que previamente enviábamos con banda estrecha, la dispersa sobre un rango de frecuencia más grande. Por ejemplo en banda estrecha podemos usar 1 MHz a 10 watts, pero en espectro disperso usamos 20 MHz a 100 mW. A través del uso de espectro disperso amplio, podemos reducir la probabilidad de que los datos sean corrompidos u obstruidos. Una señal de banda estrecha que este intentando obstruir una señal de espectro disperso, se vera frustrada en su intento debido a que la señal de banda estrecha cae en un pequeña porción del rango de frecuencia del espectro disperso. La mayoría de los datos serán recibidos libres de errores, los datos erróneos entonces serán retransmitidos usando protocolos que detecten errores en la transmisión.

2.2.3 Espectro disperso de salto de frecuencia (FHSS)

El espectro disperso de salto de frecuencia, es una tecnología de espectro disperso que usa la agilidad de la frecuencia para dispersar los datos sobre más de 83 MHz. A agilidad de la frecuencia nos referimos a la habilidad del radio para cambiar la frecuencia de transmisión abruptamente dentro de la banda de frecuencia usable. (Asignada). En el caso de WLAN con salto de frecuencia, la porción asignada en la banda de frecuencia ISM de 2.4 GHz es de 83 MHz debido a las regulación de la FCC en el estándar 802.11.

En Los sistemas de salto de frecuencia, la portadora cambia de frecuencia o salta, acorde a una secuencia seudo-aleatoria. La secuencia seudo-aleatoria es una lista de algunas frecuencias en las cuales la portadora saltara en intervalos de tiempo específicos antes de que se repita el patrón. El transmisor usa esta secuencia de saltos para seleccionar su frecuencia de salto. El transmisor se mantendrá en una frecuencia especifica, por un tiempo especifico (conocido como tiempo de morar o estadía, time dwell) transmitirá por una pequeña cantidad de tiempo para saltar a la siguiente frecuencia una vez que el periodo de tiempo haya expirado.

Hay una pequeña cantidad de tiempo durante el cambio de frecuencia en el cual el radio no esta transmitiendo llamado tiempo de salto (hop time). Cuando la lista de frecuencia ha sido agotada, el transmisor repetirá la secuencia. El tiempo de latencia es debido a que para realizar el salto, en el radio se requiere hacer los cambios necesarios para hacer esto, en algunas ocasiones se cambia a otro circuito distinto y en otras el mismo circuito es ajustado automáticamente para poder sintonizar la nueva frecuencia, todo es ocupa un tiempo que es medido en microsegundos y es llamado así, tiempo de salto (hop time). Los sistemas típicos de 802.11 en FHSS tienen tiempos de salto de entre 200 y 300 microsegundos.

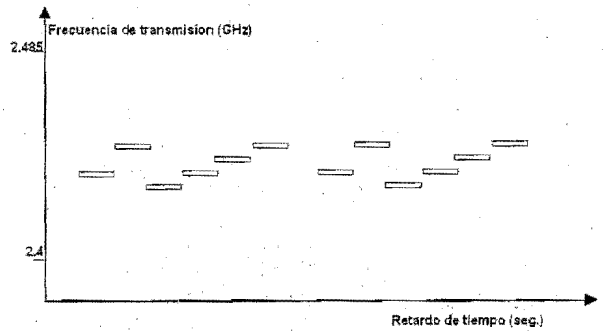


Figura 2.2.3-1 Saltos de frecuencia en FHSS

La Figura 2.2.3-1 muestra un ejemplo de saltos de frecuencia. Una vez que el radio ha transmitido la información en la lista de secuencia de frecuencias, se repite el proceso con la lista de secuencias. El radio receptor es sincronizado a la secuencia de saltos del transmisor para poder recibir la información en la frecuencia apropiada en un tiempo apropiado, la señal es entonces remodulada y usada por la computadora receptora.

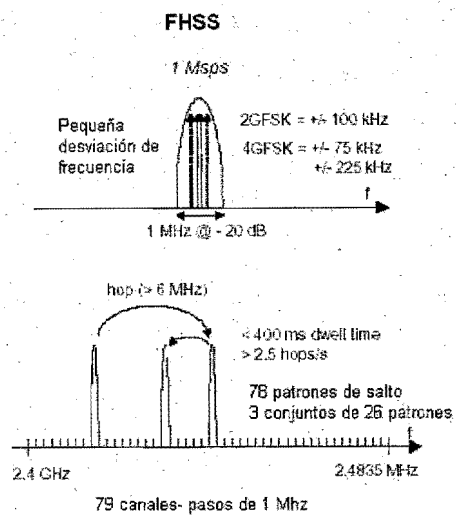


Figura 2.2.3-2 Espectro de FHSS

Como todas las tecnologías de espectro disperso, los sistemas de salto de frecuencia (FH) son resistentes, pero no inmunes a la interferencia de banda estrecha.

Los sistemas de salo de frecuencia operan usando un patrón especifico de saltos llamado canales. Los sistemas de salto de frecuencia usan típicamente los 26 patrones de salto estándar de la FCC o un subconjunto de estos. Algunos sistemas de frecuencia permiten personalizar los patrones de salto y otros también permiten sincronización entre los sistemas para eliminar por completo las colisiones en un ambiente compartido por más de un sistema con salto de frecuencia. Si no son

sincronizados los sistemas de salto de frecuencia las colisiones aumentaran a medida que aumente el tráfico o el número de dispositivos de salto de frecuencia. El tiempo de estadía (dwell time) puede se ajustado por un administrador de red WLAN para optimizar un sistema FHSS por áreas, donde hay una interferencia considerable o donde hay muy poca interferencia. En áreas donde la interferencia es muy pequeña, se puede ajusta el tiempo de estadía (dwell time grande) para una entrega de datos máxima, mientras que para área con una interferencia considerable y muchas retransmisiones debido a los datos dañados o corrompidos, es mejor ajusta el tiempo de estadia en un valor mínimo.

En la capa física de FHSS la información es primero modulada usando:

2-GFSK (Nivel 2 de FSK gausiana) para velocidades de transmisión = 1 Mbps

4-GFSK (Nivel 4 de FSK gausiana) para velocidades de transmisión = 2Mbps

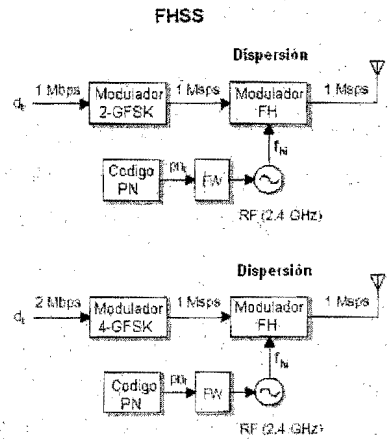


Figura 2.2.3-3 Diagrama de modulación FHSS

La frecuencia portadora (la banda ISM de 2.4 GHz, con 79 posibles canales con espacios de 1 MHz) salta de un canal a otro en un preprogramado patrón pseudos-

aleatorio, hay 78 diferentes patrones de salto (subdivididos en 3 conjuntos de 26 patrones).

Los últimos cambios del 8 de agosto del 2000 hechos por la IEEE y la FCC permiten que solo 15 saltos en u conjunto fueran requeridas, la máxima salida de potencia de un sistema es de 125 mW y puede tener un máximo ancho de banda de 5 MHz en la frecuencia portadora. Esta regla no se puede mezclar con la previa a la misma fecha. No esta permitido los traslapes de frecuencias bajo cualquier regla

2.2.4 Espectro disperso de secuencia directa (DSSS)

El espectro disperso de secuencia directa es ampliamente conocido, su popularidad es debido a la facilidad de implementación y sus altas tasas de transferencia de información. DSSS es un método de para en envió de datos en el cual los sistemas transmisores y receptores están ambos en un conjunto de frecuencias de 22 MHz. El amplio canal, permite a los dispositivos, transmitir más información a mayores tasas de transferencia que en los sistemas FHSS.

DSSS combina una señal de datos envía a una estación, con una secuencia de bits de alta velocidad, la cual es referida como "proceso de ganancia" o códigos de chip. Un alto procesamiento de ganancia, incrementa la resistencia a la interferencia de la señal. El grupo de trabajo 802.11 ha fijado su requerimiento de proceso de ganancia en 11.

El proceso de secuencia directa empieza con una portadora siendo modulada con una secuencia de código. El número de "chips" en el código determinara la cantidad de dispersión que ocurre y el número de chips por bit y la velocidad del código (en chips por segundo) determinaran la velocidad de transferencia de datos.

En la banda ISM de 2.4 GHz, la IEEE especifica el uso de DSSS a velocidades de 1 y 2 Mbps en el estándar 802.11. Bajo el estándar 802.11b se especifica a velocidades de 5.5 y 11 Mbps.

Los dispositivos 802.11b operando a 5.5 y 11 Mbps son capaz de comunicarse con los dispositivos 802.11 operando a 1 y 2 Mbps, debido a que el estándar es compatible hacia atrás con el estándar 802.11.

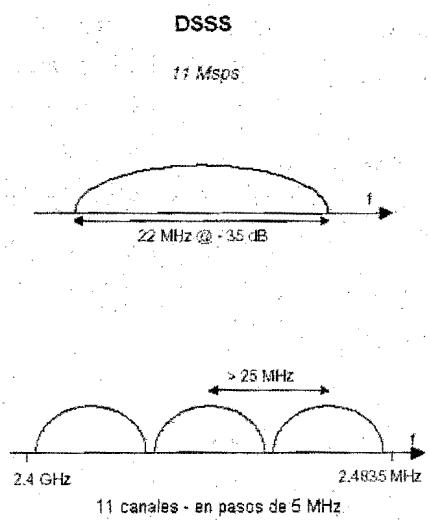


Figura 2.2.4-1 Espectro de DSSS

Distinto a los sistemas de salto de frecuencia que usan una secuencia de saltos para definir los canales, los sistemas de secuencia directa usan una definición más convencional de canales. Cada canal es una banda de frecuencia de 22 MHz de ancho y una frecuencia portadora de 1 MHz son usados similar a FHSS. El canal 1, por instancia, opera de 2.401 a 2.423 GHz (2.412 Ghz ± 11 MHz).

El estándar 802.11b especifica solo 11 canales, si hacemos cuentas de acuerdo a la Figura 2.2.4-3 todas la frecuencias adyacentes se traslapan por una cantidad significativa de espacio de espectro de RF. Las frecuencias listadas en la Figura 2.2.4-3 son el centro de los canales, adicionando o restando 11 MHz, podemos obtener los 22 MHz del canal. Por lo tanto si se usa sistemas DSSS con canales traslapados en el mismo espacio físico, se causaría interferencia entre los sistemas. Los sistemas DSSS con canales traslapados no deben colocarse en el mismo espacio físico debido a que el rendimiento se vería seriamente afectado o completamente bloqueado. Los sistemas DSSS solo podrán se ubicados físicamente si sus frecuencias no se traslapan y para que esto suceda es necesario utilizar, por ejemplo los canales 1 y 6 o los canales 2 y 7. Donde el máximo de canales permitidos en un mismo sitio seria de 3.

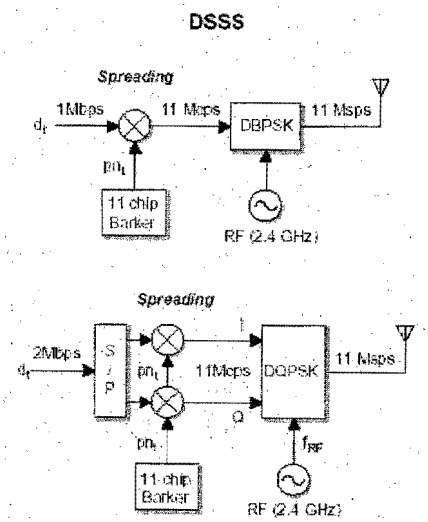


Figura 2.2.4-2 Diagrama de modulación DSSS

A continuación se lista algunos de los parámetros del estándar 802.11b.

Banda de frecuencia	2400 Mhz a 2483.5 MHz
Modulación	DBPSK a 1 Mbps
	DQPSK a 2 Mbps
	CCK a 5.5 y 11 Mbps
Medio inalámbrico	DSSS en 2.4 GHz en la banda ISM
Canales	11 canales (EE.UU. y Canadá)
Acceso al medio	CSMA/CA

Los canales de frecuencia del estándar 802.11b son los siguientes:

Canales de frecuencia para DSSS

ID de Canal	Frecuencias GHz (FCC)	Frecuencias GHz (ETSI)
1	2.412	N/A
2	2.417	N/A
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

Figura 2.2.4-3 Canales de frecuencia DSSS

Igual que los sistemas de salto de frecuencia, los sistemas de secuencia directa también son resistentes a interferencias de banda estrecha debido a que sus características de espectro disperso. Una señal de DSSS es mas susceptible a las interferencias de banda estrecha que una señal de FHSS, debido a que la banda de DSSS es mas pequeña (22 Mhz mientras que FHSS utiliza 79 MHz) y a que la información es transmitida a lo largo de la banda simultáneamente. Con la agilidad de frecuencia de FHSS y su amplia banda de frecuencia, se asegura que la interferencia solo influya por una pequeña cantidad de tiempo, dañando solo una pequeña porción de los datos.

2.3 Técnicas de acceso

Para que un usuario pueda acceder al canal de un sistema de radio requiere que este disponible el canal. Si el número de canales disponibles para todos los usuarios de un sistema de radio es menor que el número de posibles usuarios, entonces a este sistema se le llama sistema de radio troncal izado.

La troncalización es el proceso por el cual los usuarios comparten un determinado número de canales de forma ordenada. Los canales compartidos funcionan debido a que podemos estar seguros que la probabilidad de que todo el mundo quiera un canal al mismo tiempo es muy baja.

Un sistema de telefonía celular troncal izado, es aquel en el que hay menos canales al mismo tiempo.

El acceso se garantiza dividiendo el sistema en uno o más de sus dominios: frecuencia, tiempo o codificación.

2.3.1 Acceso múltiple por división de frecuencia (FDMA)

FDMA asigna a los usuarios un canal de un conjunto limitado de canales ordenados en el domino de la frecuencia. Los canales de frecuencia son asignados a los

sistemas por los organismos reguladores como la Cofetel en el caso de México, de acuerdo con las necesidades de la sociedad.

Cuando hay más usuarios que el suministro de canales de frecuencias pueda soportar, se bloque el acceso de los usuarios al sistema.

Los sistemas FDMA muy grandes tienen más de un canal de control para manejar todas las tareas de control de acceso. Una característica importante de los sistemas FDMA es que una vez que se asigna una frecuencia a un usuario, es usada exclusivamente por ese usuario hasta que se libere el recurso.

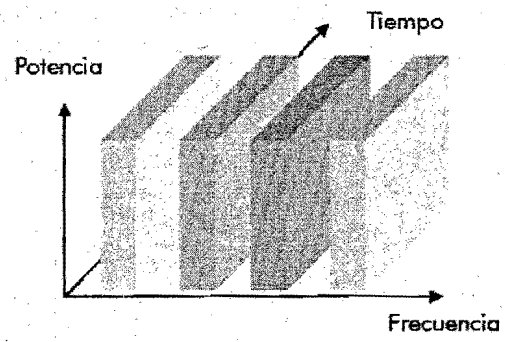


Figura 2.3.1-1 FDMA

2.3.2 Acceso múltiple por división de tiempo (TDMA)

TDMA es una tecnología de radios de transmisión digital, que permite a un numero de usuarios acceder a un canal de radiofrecuencia sin que se interfieran, ya que se colocan en una ranura de tiempo (del un mismo canal de radiofrecuencia) distinta para cada usuario, dentro del canal.

Los usuarios acceden a un canal de acuerdo con un esquema temporal, es decir en el dominio del tiempo. Los sistemas celulares que emplean técnicas TDMA, siempre

usan TDMA sobre una estructura FDMA. Un sistema TDMA puro, tendría solo una frecuencia de operación, y no seria un sistema útil.

Las modernas técnicas de codificación de voz, reduce mucho el tiempo que se lleva en transmitir mensajes de voz, eliminando la mayoría de la redundancia y periodos de silencio en las comunicaciones de voz.

Otros usuarios pueden compartir el mismo canal durante los periodos en los que no se utiliza. A todos los usuarios que comparten la misma frecuencia se les asigna un slot de tiempo, que se encuentra en la misma trama.

Por ejemplo: un spot puede ser de 577 as, y si el canal puede soportar a 8 usuarios por canal de frecuencia, cada usuario tiene uso del canal (mediante su slot) capa 4.615 ms (8 * 577 µs = 4.615 ms).

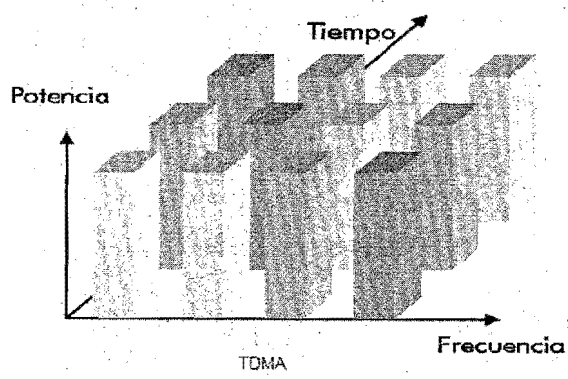


Figura 2.3.2-1TDMA

2.3.3 Acceso múltiple por división de código (CDMA)

CDMA es un método en el cual los usuarios comparten las frecuencias al mismo tiempo y son canalizados o reconocidos, asignado códigos únicos. Las señales se

separan en el receptor utilizando una correlación que solo acepta energía de los canales deseados. Las señales no deseadas se consideran ruido.

CDMA esta basado en la tecnología de espectro disperso.

El espectro disperso tiene dos modalidades: salto de frecuencia o secuencia directa.

Es una técnica de modulación en la cual la información modulante se esparce o se expande a través de un ancho de banda más amplio que el contenido de frecuencia de la información original. El método del espectro disperso toma la señal de entrada, la mezcla y la parte en un amplio rango de frecuencia. La señal dispersa posee un mayor ancho de banda que la original. El receptor reconoce la señal dispersa, la recoge y la comprime de nuevo para devolverla a su forma inicial. El método del espectro disperso posee una alta seguridad y es inmune a la interferencia.

2.3.4 Principio CDMA

Todas las estaciones de la red pueden transmitir continuamente ocupando el mismo ancho de banda

Se produce interferencia entre las transmisiones de las diferentes estaciones.

El receptor resuelve la interferencia identificando la firma de cada transmisor.

La firma es una secuencia binaria, llamada código, que se combina con la información a transmitir para cada transmisor. Debe distinguirse fácilmente de los demás códigos e incluso de una copia retardada de si mismo. Los bits del código se denominan chips. Para transmitir el código y la información se requiere mas ancho de banda.

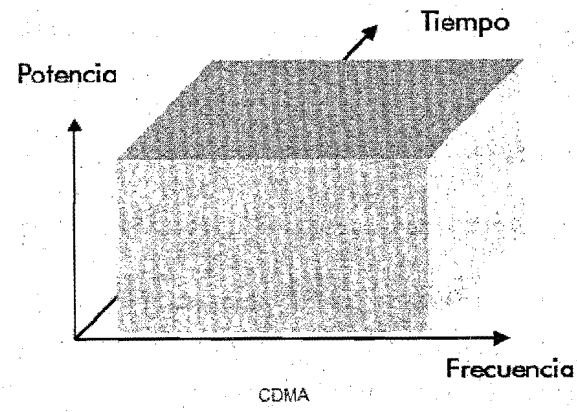


Figura 2.3.4-1 CDMA

2.3.5 CDMA de acceso expandido (B-CDMA)

La compañía interdigital ha desarrollado una modalidad de CDMA basado en espectro extendido, y lo denomino Broadband code division múltiple access (B-CDMA). Esta enfocado a redes punto multipunto y provee a los usuarios acceso a la red publica telefónica bajo demanda, empleando señales de radio especiales, que transportan voz, datos y servicios de facsímile.

Emplea un ancho de banda lo suficientemente grande como para que solo una pequeña parte de la señal se degrade por multipath fading, esto aunado a las técnicas usadas por interdigital permite la recuperación de la señal degradada.

2.3.6 CDMA de banda ancha (WCDMA)

Es el método de acceso por división de códigos de banda ancha, capaz de manejar anchos de banda de 2 Mbps o más con la finalidad de tener acceso a toda la gama

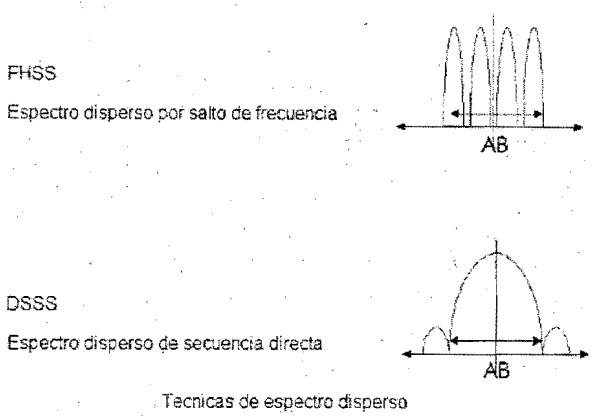


Figura 2.3.6-1 Espectro disperso

de servicios de la red ISDN de banda ancha, e incluso al Internet a través de enlaces inalámbricos.

Se define como la tecnología a emplearse para la 3G de sistemas de telefonía inalámbrica en los próximos años. Entre todas las tecnologías consideradas para la interfaz de aire de UMTS.

2.3.7 Multiplexión por división en longitud de onda (WDM).

Para los canales de fibra óptica se utiliza una variante de la multiplexión por división en frecuencia llamada WDM (wavelength división multiplexing, multiplexión por división en longitud de onda). Dos fibras llegan juntas a un prisma (o para ser mas precisos a una rejilla de difracción), cada una con su energía en una banda diferente. Los haces pasan a través del prisma o rejilla, y se combinan en una misma

fibra compartida para ser transmitida a un destino diferente, donde se dividirán de nuevo.

2.3.8 OFDM.

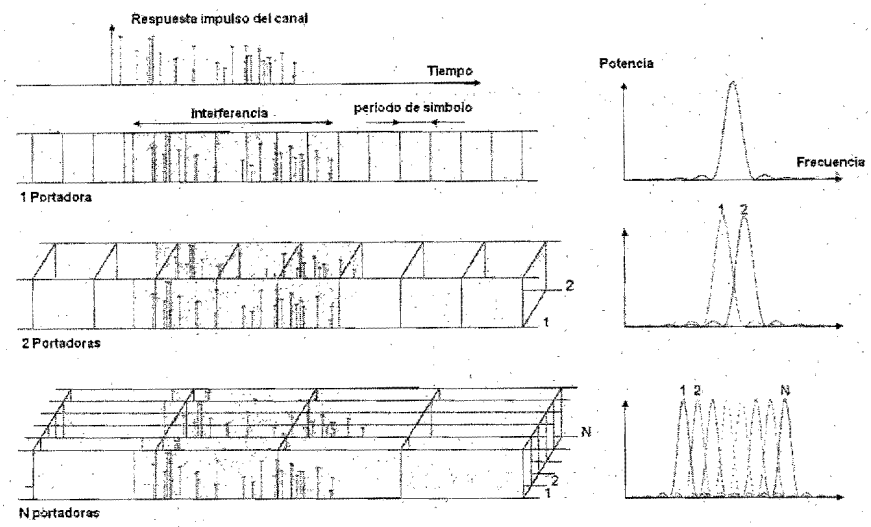


Figura 2.3.8-1 OFDM

Supongamos que **N** es el número total de portadoras del sistema, f_0 es la frecuencia de la primera de ellas, y **T** es el período de símbolo de cada flujo de datos.

Entonces, las frecuencias de las **N-1** portadoras restantes vienen dadas por la relación $f_k = f_0 + k/T$, con **k = 1, 2,..., N-1**. Es decir, que la separación entre portadoras adyacentes es de **1/T**, el inverso del período de símbolo.

La señal recibida en la cabecera es la suma de las **N** señales individuales.

La separación de **1/T** Hz. garantiza la ortogonalidad, y la señal recibida puede ser de-multiplexada usando una transformada discreta de Fourier (DFT). La estación de cabecera conoce perfectamente la información relativa a la sincronización y

ubicación de frecuencia de las portadoras digitales ya que es ella misma la que se la proporciona a todas las unidades de abonado a través del canal descendente.

Capitulo 3 Redes de computadoras

3.1 Redes de computadoras

Debido al tremendo impacto de las computadoras y de las redes de computadoras, estas dos son dos áreas que prácticamente tienen que ver con cualquier área que requiera manejar información, almacenar, procesar y distribuir información. Al hablar de información son referimos a datos, audio y video (fijo como imágenes y video en movimiento como películas). Las redes de computadoras nos permiten compartir recursos, esto es información y servicios de red como impresoras compartidas, conexiones a Internet, etc. También permiten interconectar redes que físicamente se encuentran separadas por algunos cientos de metros y hasta cientos de kilómetros de distancia entre ellas, pueden ser conectadas dos a más redes para formar una gran red. Actualmente las redes están en muchas empresas grandes y pequeñas, y en algunas casas ya hay incluso algunas redes pequeñas. La tendencia indica que estas se seguirán extendiendo alrededor del mundo en un sin fin de aplicaciones, permitiendo a sus usuarios incrementar su productividad, ampliar su medios de comunicación, compartir recursos, disponer de información, etc.

Las redes de computadoras han estado evolucionando tanto a nivel hardware como a nivel software. A nivel software las aplicaciones se han hecho mas robustas permitiendo hacer prácticamente cualquier cosa dentro de una computadora como: diseño grafico, manejo de bases de datos, diseño asistido por computadora, fabricación asistida por computadora, correo electrónico, Internet, edición de audio y video, etc. Los sistemas operativos que son la base para que se ejecute un programa también han evolucionado ahora hay sistemas operativos de 32 bits, y ya hay propuestas de sistemas operativos de 64 bits para aplicaciones mas avanzadas como la investigación. En el campo del hardware las computadoras y sus componentes también han evolucionado, ahora cuentan con nuevas interfaces mas rápidas como USB versión 2.0 de 480 Mbps, Firewire, discos duras con interfaces mas rápidas como SATA, interfaces de video como AGP, monitores de LCD; monitores de plasma; monitores de DLP, conexiones de red 10/100/1000 Mbps, MODEM con estándar V.92, lectores y grabadores de disco ópticos (CD-RW y DVD-

RW), y la lista continua. La industria de la computación sigue su camino paralelo a la industria de las comunicaciones. En el campo de las comunicaciones, ahora dispones de muchas tecnologías de ínter conectividad a diferentes niveles que nos permiten conectar dos o mas redes prácticamente en cualquier lugar del mundo, usando ya sea líneas telefonía, cable UTP, cable coaxial, fibra óptica y las ondas electromagnéticas en el espacio libre como medio de transporte. Se hable de tecnologías como X.25, Frame Relay, ATM, ISDN, ADSL, E1 en enlaces de radio, GPRS, enlaces satelitales, etc. Que pueden ser usados por los clientes para interconectar sus redes.

Las redes de computadoras se han vuelto el equipo mas versátil jamás inventado por el hombre, en sus inicio solo era capas de manejar información de texto y datos de operación matemáticas ya sea financieras o científicas. Hoy en día a través de las redes de computadores de procesa información que puede ser texto, datos numéricos de operaciones matemáticas, audio, imágenes, video, procesamiento de información como temperatura, velocidad, aceleración, fuerza, volumen, etc. La computadora ahora esta en oficinas, centros de fabricación, en el automóvil, en naves espaciales, en equipo de computo móvil (DPA), etc.

Actualmente las redes de computadoras LAN, en su mayoría se implementan con cableado CAT5 para ethernet a 10/100 mbps y hay algunas a 1000 Mbps con su respectivo cable. Mas sin embargo las redes de computadoras inalámbricas están tomando fuerza, lo que se consideraba solo una curiosidad experimentada por sus diseñadores, sin ningún estándar que los respaldara, ahora disponemos de prácticamente de 4 estándares internacionales para redes inalámbricas, todos de la serie 802.11 del IEEE, y ya hay propuestas para mejorar estas redes en cuando a rendimiento, seguridad y calidad de servicio. Por lo que podemos contar que las redes ya no serán exclusivamente por cable y podemos pensar que las redes inalámbricas llegaron para quedarse.

Hay varias definiciones aceptadas en la industria para "redes de computadoras", quizás la más simple sea la siguiente: una red de computadoras es un conjunto de

computadoras conectadas mediante una o más vías de comunicación. La vía de comunicación puede ocupar cualquier medio de transporte como ya se menciono anteriormente. La red existe para cumplir un determinado objetivo: la transferencia e intercambio de información entre computadoras. Este intercambio de datos es la base de muchos de los servicios basados en computadoras que actualmente usamos en nuestra vida diaria como cajeros automáticos, correo electrónico, Internet, compras en tiendas de autoservicio y muchas más.

Las redes de computadoras proporcionan importantes ventajas a nivel empresarial como a nivel personal.

Las redes de computadoras permiten interconectar varias computadoras que están situadas geográficamente en varias ubicaciones alrededor de un país o incluso del mundo.

Las redes de computadoras permiten compartir recursos informáticos, como bases de datos, y recursos de cómputo, permitiendo enviar el procesamiento a otro centro de cómputo que se encuentre menos saturado.

facilitan la tolerancia a fallos al permitir tener mas de un servidor dedicado a una tarea, cuando un servidor falla es posible dar el servicio con un servidor que se encuentra ubicado en otro lugar geográfico.

el uso de redes permite disponer de un entorno de trabajo mas flexibles los empleados pueden trabajar desde lugares remotos utilizando una computadora para conectarse a su empresa, usando conexiones telefónicas para conexiones punto a punto o conexiones a través de Internet usando VPN´s.

ETD (equipo terminal de datos) es un término genérico usado para designar al equipo de usuario final donde reside la aplicación, habitualmente una computadora de escritorio, portátil o una terminal. La finalidad de las redes de comunicaciones es conectar ETD de forma que puedan compartir recursos, intercambiar datos, procesar información de forma conjunta. Las redes de comunicaciones proporcionan

comunicaciones lógicas y físicas las aplicaciones y los archivos utilizan el canal físico para realizar comunicaciones lógicas, las comunicaciones lógicas son cuando los ETD no necesitan saber nada de los aspectos físicos del proceso de comunicación. La función de un ETCD (equipo terminal de comunicación de datos) es conectar los ETD al canal o línea de comunicación, la función primordial de los ETCD es servir de interfaz entre el ETD y la red de comunicaciones. Las interfaces se especifican y establecen mediante protocolos, los protocolos establecen la forma en la que los ETD y la elementos de comunicaciones intercambian la información entre si. Tipicamente para soportar una aplicación de usuario final se requieren de varios niveles de interfaces y protocolos.

Los ETD y los ETCD se pueden conectar de dos formas:

Punto a punto, en esta configuración solo hay dos ETD conectados a la línea de comunicación

Multi-punto, en esta configuración hay mas de dos ETD conectados a un mismo canal.

Los ETD pueden intercambiar tráfico de comunicación de tres maneras:

Simplex

Half-duplex

Full-duplex.

3.2 Modelo de referencia OSI

OSI (interconexión de sistemas abiertos) conocido como modelo de referencia OSI, describe como se transfiere la información desde una aplicación de software en una computadora a través del medio de transmisión, hasta la aplicación de software en otra computadora. OSI es un modelo compuesto de siete capas, en cada una de ellas se especifican funciones de red muy particulares. OSI divide las funciones

implicadas en la transferencia de información entre computadoras, en siete grupos de tareas más pequeños y fáciles de manejar. A cada una de las siete capas se asigna una tarea o grupo de tareas. Cada capa es razonablemente individual, de tal manera que cada una de esta se puede implementar de manera independiente sin necesidad de afectar a las otras. Esto permite que las soluciones ofrecidas por una capa se puedan actualizar sin afectar a las demás.

3.2.1 Capas superiores y capas inferiores

Las capas del modelo de referencia OSI se pueden dividir en dos categorías.

Las capas superiores del modelo OSI tienen que ver con la aplicación y en general están implementadas solo en software. La capa superior, la de aplicación, es la más cercana al usuario final. Tanto los usuarios como los procesos de la capa de aplicación interactúan con aplicaciones de software que contienen un componente de comunicación. El termino capa superior se usa a veces para referirse a cualquier capa que este sobre otra capa en el modelo OSI.

Las capas inferiores de modelo OSI, manejan lo concerniente a la transferencia de datos. Las capas físicas y de enlace de datos se encuentran implementadas en hardware y software. En general las otras capas inferiores están implementadas únicamente en software.

El modelo de referencia OSI proporciona un marco conceptual para la comunicación entre computadoras, pero el modelo en si mismo no es un método de comunicación. La comunicación real se hace posible al utilizar protocolos de comunicación tales como TCP/IP.

Cualquiera de las capas del modelo OSI se comunica con 3 capas del mismo modelo, la superior e inferior a ella y su igual pero en el equipo con la que se conecta o envía datos de redes de comunicaciones

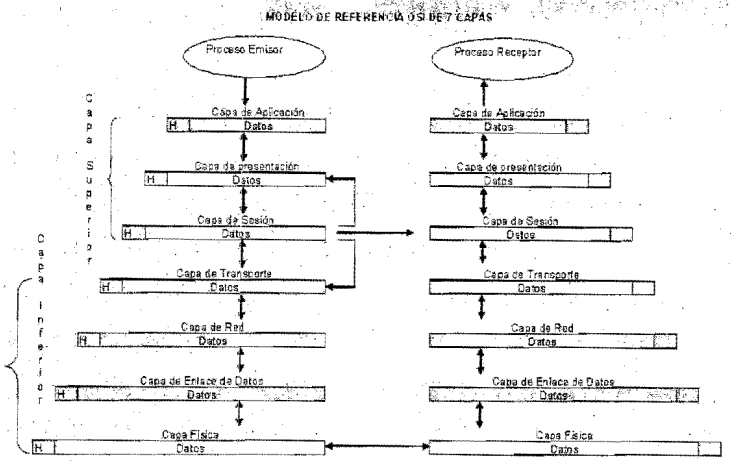


Figura 3.2.1-1 Modelo de referencia OSI

3.2.2 Capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimientos y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de redes de comunicaciones. Las especificaciones de la capa física definen características como niveles de voltaje, temporización de cambios de voltajes, velocidades de transferencia de información, distancias máximas de transmisión y conectores físicos. Las implementaciones de la capa física se pueden categorizar como especificaciones LAN o WAN. En implementaciones de interconexión existen diferentes tipos de interfaces como son:

1. EIA/TIA RS-232, es una interfaz de transmisión serial definido por la EIA y la TIA que soporta velocidades hasta de 64 kbps, es utilizado en comunicación de equipos ETD y ETCD.
2. 802.3 Es un protocolo de capa física que define características eléctricas, mecánicas, temporización y de operación de la interfaz. La interfaz mecánica de esta es un conector conocido ampliamente como RJ-45 de 8 patas. Fast Ethernet, al igual que Ethernet utilizan la misma conexión

física. Es ampliamente utilizado en ruteadores para el acceso a Internet con modems ADSL (prodigy infinitum)

3. V.35 es un estándar de la ITU-T que describe un protocolo de capa física usado para la comunicación entre dispositivos de acceso de red, fue diseñado originalmente para MODEM sincronos de 48 kbps.
4. G.703 es un estándar que permite comunicaciones en múltiplos de canales de 64 kbps para transmitir canales de voz sin comprimir o cual otro tipo de información digital. Es utilizado ampliamente en enlaces de comunicación de voz como los E1 (estándar europeo) y T1 (estándar americano). El G.703 utiliza cable coaxial de 75 ohms y conectores tipo BNC.
5. EIA/TIA 612/613 o HSSI es una interfaz serial de alta velocidad DTE/DCE con una transferencia máxima de 52 Mbps con lo cual es posible manejar velocidades de hasta un T3 (45 Mbps) en la parte WAN. HSSI utiliza un conector de 50 patas tipo sub-miniatura.

La capa de enlace de daros proporciona el transito confiable de datos a través del enlace de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes características de red y de protocolo, incluyendo direccionamiento físico, topología de red, la notificación de error, la secuencia de tramas y el control de flujo. El direccionamiento físico (a diferencia del direccionamiento de red), define como se nombran los dispositivos en la capa de enlace de datos. Que con frecuencia definen la forma en que se conectaran físicamente los dispositivos. La notificación de error alertara a los protocolos de las capas superiores cuando se presenta un error en la transmisión y la secuencia de tramas de datos reordena las que se han transmitido fuera de secuencia. Finalmente el control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con más tráfico del que pueda manejar simultáneamente. El IEEE a subdividido la capa de enlace de datos en dos capas: LLC (control de enlace lógico) i MAC (control de acceso a medios). La sub-capa LLC de la capa de enlace de datos administra las comunicaciones entre los dispositivos unidos por un enlace individual de red. La sub-capa LLC. La sub-capa MAC de la

capa de enlace de datos administra el protocolo de acceso al medio de transmisión físico de la red. Las especificaciones IEEE MAC define las direcciones MAC, las cuales permiten a varios dispositivos identificarse de manera única entre si en la capa de enlace de datos.

3.2.3 Capa de red

La capa de red proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos combinarse en una red. Esto se logra a través del direccionamiento lógico (opuesto al direccionamiento físico) de los dispositivos. La capa de red soporta servicios orientados y no orientados a conexión de los protocolos de las capas superiores. Los protocolos de red pueden ser clasificados en protocolos de ruteo y protocolos ruteables. Un ejemplo de protocolos ruteables sea el protocolo IP y IPX, IP es ampliamente utilizado en redes Ethernet e Internet. Los protocolos de ruteo operan solo dentro de los dispositivos de ruteo sobre la capa de red y estos pueden ser clasificados como: IGP y EGP, los protocolos IGP son aquellos protocolos que se utilizan dentro de un sistema autónomo de redes administrados bajo en mismo centro de control. Los protocolos IGP (protocolos de compuerta interior) son:

1. RIP (protocolo de información de ruteo)
2. OSPF (Protocolo de abrir primero la ruta mas corta)
3. IGRP (Protocolo de ruteo de compuerta interior)
4. EIGRP (Protocolo de ruteo de compuerta interior extendido)

Los protocolos EGP son los protocolos que nos permiten interconectar dos o más sistemas autónomos como ejemplo de protocolo EGP (protocolo de compuerta exterior) es:

1. BGP (protocolo de compuerta limite)

3.2.4 Capa de transporte

La capa de transporte implementa servicios confiables de datos entre redes, transparentes a las capas superiores. Entre las funciones habituales de la capa de transporte se encuentran el control de flujo, el múltiplexaje, la administración de los circuitos virtuales y la verificación y control de errores.

El control de flujo administra la transmisión de datos entre los dispositivos para que el dispositivo transmisor no envié más datos de los que pueda procesar el dispositivo receptor. El múltiplexaje permite que los datos de diferentes aplicaciones sean transmitidos en un enlace físico único. Es la capa de transporte la que establece, mantiene y termina los circuitos virtuales. La verificación de errores implica la creación de varios mecanismos para detectar los errores en la transmisión, en tanto que la recuperación de errores implica realizar una acción, como solicitar la retransmisión de los datos para resolver cualquier error que pueda ocurrir.

3.2.5 Capa de sesión

La capa de sesión establece administra y finaliza sesiones de comunicación entre las entidades de la capa de presentación. Las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red. Estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión

3.2.6 Capa de presentación

Esta capa proporciona una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea legible por la capa de aplicación de otro sistema. Los formatos de presentación de datos comunes o el uso de formatos estándar de texto, imagen, sonido y video, permiten el intercambio de datos de aplicación entre diferentes tipos de sistemas de computadoras.

3.2.7 Capa de aplicación

La capa de aplicación es la capa OSI que esta cerca al usuario. Esta capa proporciona servicios de red a las aplicaciones del usuario, esta capa interactúa con las aplicaciones de software que un componente de comunicación. Dichos programas están fuera del alcance del modelo OSI. Las funciones de la capa de aplicación incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de recursos y la sincronización de la comunicación. Esta capa es diferente a las otras capas del modelo OSI debido a que esta no proporciona servicios a otra capa superior.

3.3 Topologías de redes.

Una configuración de red se denomina topología de red. Por lo tanto, la topología establece la forma (conectividad física) de la red. Al establecer una topología de red se debe considerar los siguientes objetivos:

Proporcionar la máxima fiabilidad a la hora de establecer el tráfico (por ejemplo mediante varias rutas distintas).

Realizar las rutas utilizando el costo mínimo entre los ETD transmisores y receptores. Los costos puedes ser de tiempo o económicos. Proporcionar un medio de comunicación que sea acorde a las necesidades de la aplicación y de las posibilidades de la empresa o usuario, esto es para mantener los costos de comunicación lo mas bajos posibles.

Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo.

Minimizar la longitud real del canal entre los componentes que se comunican, para lo cual se debe de encaminar el tráfico por la ruta que utilice el menor número de componentes de comunicación.

Para esto existen varias configuraciones de red que en su mayoría están ligadas a ciertas tecnologías de red.

3.3.1 Topología jerárquica

La topología jerárquica es una de las más utilizadas hoy en día, la propia topología proporciona un punto de concertación para el control y resolución de errores. En la mayoría de los casos, el ETD (equipo terminal de datos) de mayor jerarquía es el que controla la red. El flujo de datos entre los ETD lo inicia el ETD de mayor jerarquía. En algunos diseños, el concepto de control jerárquico se distribuye, donde se proponen métodos para que algunos ETD subordinados controlen los ETD por debajo ellos en la jerarquía. De esta manera se reduce la carga de trabajo al ETD de mayor jerarquía. La topología jerárquica también se denomina "red vertical" o "red en árbol"

3.3.2 Topología horizontal (bus)

En la topología horizontal o de bus, el control del tráfico es relativamente simple, ya que el bus permite que todas las estaciones (computadoras) reciban la transmisión. Es decir cada estación es capaz de transmitir su información y esta llegara a cada estación que esta conectada al bus. El principal inconveniente de esta topología es que habitualmente solo existe un único canal de comunicaciones al que se conectan todos los dispositivos de al red. En consecuencia se falla el canal, toda la red deja de funcionar.

3.3.3 Topología de estrella

En la topología de estrella, todo el tráfico seria del centro de la estrella. Donde en el centro de la estrella se encuentra un dispositivo que controla completamente el tráfico generado por los ETD. El nodo central es el responsable de encaminar el trafico entre los componentes y a su vez responsable de ocuparse se las fallas. La localización de averías es relativamente simple en esta configuración, ya es posible aislar las líneas para identificar la falla. Sin embargo dado que se dispone de un nodo central por donde cursa todo el trafico, es como encontrar cantidades de trafico

considerables, para esto solo se dispone de nodo de reserva lo que incrementa considerablemente la fiabilidad del sistema.

3.3.4 Topología en anillo

La topología en anillo recibe su nombre del aspecto circular del flujo de datos. En muchas ocasiones el flujo de datos va en una sola dirección. Es decir una estación recibe la señal y la envía a la siguiente estación del anillo. La topología en anillo es muy atractiva debido a que los cuellos de botella son mucho más raros. El principal inconveniente de esta topología es que un único canal une todos los componentes del anillo. Si falla el canal entre los nodos, falla toda la red. Como consecuencia de esto algunos sistemas incorporan canales de reserva o anillos dobles.

3.3.5 Topología en malla

El principal atractivo de la topología en malla es su relativa inmunidad a problemas de fallos y cuellos de botella. Dado la multiplicidad de caminos entre los ETD, es posible encaminar el tráfico evitando componentes que fallan o nodos ocupados. Aunque esta solución es costosa, algunos usuarios prefieren la gran fiabilidad de la topología en malla frente a las otras.

En términos generales al hablar de topología nos referimos a la forma en que física esta conectada la red de comunicación entre dos o mas computadoras o redes.

Muchas de las topologías de una red empresarial o residencial, dependerán de las tecnologías a ser utilizadas.

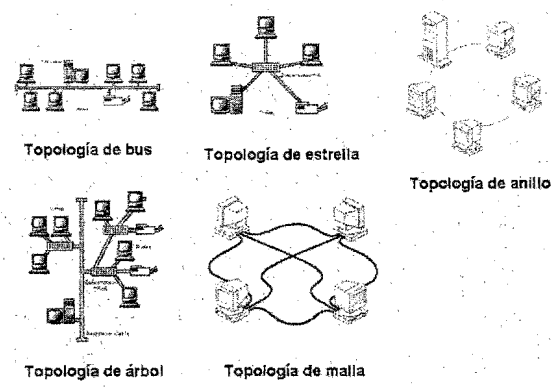


Figura 3.3.5-1 Topologías de red

3.3.6 Servicios orientados a conexión y sin conexión

Los medios de comunicaciones utilizados para conectar dos o más dispositivos o redes, ya sea que estos sean medio contratados o propios de la empresa o persona pueden estar orientados a dos diferentes tipos de servicios:

El servicio orientado a la conexión, es aquel en el cual primero se estable una conexión, se usa para el envió de datos y después se libera la conexión. Esta conexión es establecida desde el origen hasta el destino a donde queremos enviar los datos.

El servicio sin conexión, como su nombre lo dice no realiza alguna conexión, solo envía los datos (en forma de paquetes) marcando los datos con la dirección destino pero sin hacer uso de algún protocolo que mantenga una conexión entre los puntos origen y destino.

Capas de comunicación del modelo OSI o de cualquier otra forma, pueden ofrecer dos tipos diferentes de servicios

3.3.7 Códigos de sincronización

En transmisiones de larga distancia, es económicamente más rentable incorporar la temporización dentro de la propia señal que se transmite, en vez de utilizar un canal diferente para la señal de reloj, esto es lo que se conoce como un código auto sincronizado. Los códigos no auto sincronizados presentan el problema de que el reloj y los datos pueden resultar alterados al propagarse por canales diferentes. Es posible por ejemplo, que la señal de reloj se haga algo más rápida o más lenta. Si esto ocurre, el receptor tendrá dificultades para sincronizarse con los datos transmitidos.

Con el uso de códigos auto sincronizados, el receptor puede verificar por si mismo si esta muestreando la señal en el momento exacto en el que recibe los bit de datos. Para ello se requiere que la señal recibida cambie su estado muy seguido y de manera regular. Los mejores códigos son los que causan cambios muy frecuentes en el estado de la señal recibida por el receptor, ya que estos cambios, permiten al receptor ajustarse continuamente a la señal.

3.4 Códigos de línea

Básicamente, existen dos formas de enviar señales por una línea de transmisión. Podemos optar por enviar la información directamente, sin ningún tipo de modificación, en forma digital o bien pueden componerse con una onda de frecuencia más alta que sirve de transporte.

En el primer caso se habla de transmisión en banda base. La principal ventaja que ofrece es la sencillez y economía del proceso. Su principal inconveniente es la atenuación introducida por la línea a este tipo de señales que provoca importantes distorsiones. La transmisión en banda base admite distintos tipos de codificaciones, formas de representar la información binaria que en este caso nos referimos a los códigos de línea.

En el segundo caso se trata de enviar señales moduladas sobre ondas portadoras de determinadas frecuencias.

La transmisión de datos en forma digital a través de cualquier medio de transmisión implica una cierta codificación. A esta codificación que se realiza sin que exista una modulación se le conoce como un código de línea en banda base.

Los códigos de línea son adecuaciones de la señal eléctrica para ser enviada sobre el medio de transmisión ya sea este un alambre coaxial, alambre trenzado o el espacio libre, y poder ser procesada por los sistemas de comunicaciones. Los códigos de línea tienen diferentes clasificaciones entre las cuales destaca la siguiente:

Nombre	Unipolar/bipolar
NRZ	unipolar
RZ	unipolar
AMI	bipolar
HDB-3	bipolar
CMI	bipolar
PST	bipolar
DICODE	bipolar
B3ZS	bipolar

Al hablar de unipolar o bipolar nos referimos a tipo de excursión que hace la señal, las señales unipolares son aquellas que solo van de cero a un valor positivo sin pasar esta señal al cuadrante negativo, por el contrario las señales bipolares toman tanto valores positivos como negativos cruzando por cero.

3.4.1 Código RZ

RZ acrónimo de "Return to Zero" es un código con retorno al nivel cero, en el cual durante el paso de un bit a otro bit del mismo signo (paso de "1" a "1" ó de "0" a "0") se vuelve siempre al nivel cero.

EL código denominado RZ (retorno a cero), el 1 lógico viene representado por un pulso positivo, mientras que la ausencia de pulso representa un cero.

3.4.2 Código NRZ

NRZ acrónimo de "Non Return to Zero", es un código sin retorno al nivel cero. En este código, durante el paso de un bit a otro bit del mismo signo (paso de "1" a "1" ó de "0" a "0") no se vuelve al nivel cero, en contraposición al código RZ.

El código NRZ (Non Return to Zero) es similar al RZ pero sólo se obtienen impulsos para los cambios de "1" a "0" y de "0" a "1".

Este código necesita sincronización externa. La pérdida de sincronización no se detecta y produce información errónea. En el caso de producirse un error, quedan afectados todos los bits posteriores. Su ventaja es que permite una gran densidad de grabación.

En las transmisiones en banda base se utiliza directamente señales digitales de forma directa, por ejemplo 5 voltios indican "1" y 0 voltios indican "0". Existen dos formas básicas de código NRZ y estas son NRZ bipolar y NRZ unipolar. El código NRZ unipolar representa un 1 lógico con una tensión positiva y un 0 lógico con cero volts, mientras que el código NRZ bipolar representa un 1 lógico con una tensión positiva y un 0 lógico con una tensión negativa.

3.4.3 Código AMI

Código por inversión de marcas alternas. Dado que el código NRZ no es conveniente para transmitir a largas distancias (por su contenido de CD), se ha

desarrollado el código AMI para su uso en la transmisión en largas distancias. El propósito de este código es el de reducir el continuo nivel de CD en la línea a 0 volts. En este código un "0" será representado por 0 volts y un "1" por un voltaje alternado positivo o negativo. Al invertir la dirección de las marcas consecutivas, el promedio de componente CD en la línea cae a 0 volts. Como resultado, este código es conveniente para transmisor a larga distancia. Sin embargo este código no transmite el sistema de reloj, el receptor debe reconocer y seleccionar la tasa del reloj de entrada explorando por transiciones en la cadena de bits de entrada. Si se tiene una serie de bits que son iguales a "0", el receptor ya no puede reconocer la velocidad del reloj, por que se tiene un nivel continuo de CD (0 volts) en la línea. Para resolver este problema, se ha desarrollado otro código llamado alta densidad bipolar exceso 3 (HDB3)

3.4.4 Código HDB3

Este código inserta pulsos de violación cuando llegan sucesivamente mas de 3 ceros. El lado transmisor inserta pulsos de violación, los cuales pueden ser detectados por el receptor, el lado receptor eliminara los pulsos de violación.

Los pulsos de violación son insertados dependiendo del numero de pulsos que han pasado y dependiendo del signo del ultimo pulso de información. Él número de pulsos puede ser par o impar. El signo del último de información puede ser negativo o positivo.

3.4.5 Código CMI

En el código CMI (código de inversión de marcas codificadas) los "1" se siguen alternando y dura un ciclo de reloj, mientras que los ceros duran la mitad del reloj.

3.4.6 Códigos PST (Paired Selected Ternary)

La codificación de señal digital es desarrollada de acuerdo con las siguientes reglas:

Cuando un "1 0" o un "0 1" aparece, el modo mostrado arriba es alternado de modo 1 a modo 2 alternativamente. Pulsos positivos y negativos son asignados a cada nivel lógico "1" basado en las reglas de codificación.

Codigos PST

Patron de la señal	reglas de codificacion	
para cada dos bits	modo 1	modo 2
"1 1"	+V, -V	+V, -V
"1 0"	+V, 0	-V, 0
"0 1"	0, +V	0, -V
"0 0"	-V, +V	-V, +V

Figura 3.4.6-1 Códigos PST

3.4.7 Códigos Dicode

Cuando el nivel de señal es como el pulso continuo precedente, es asignado "0". Esto es cuando se presenta de forma continua " 1 1" o "0 0" se asigna un 0.

Cuando el nivel de la señal del primero y segundo pulso son "0" y "1" respectivamente es asignado un +V.

Cuando el nivel de la señal del primero y segundo son "1" y "0" respectivamente, es asignado un –V.

3.4.8 Código bipolar con 3 ceros de sustitución (B3ZS)

Cuando menos de 3 bit continuos de "0" en sucesión, las reglas del código AMI son aplicables.

Cuando más de 3 bits continuos sucesivamente, la señal "000" es remplazada con señales "B0V" o "00V", donde

El pulso B: pulso lógico "1" en correspondencia con las reglas de la codificación bipolar.

Pulsos V: pulso lógico "1" (pulso de violación) no esta de acuerdo con las reglas de codificación bipolar.

El uso de "B0V" o "00V" depende del número de pulsos B contenidos entre los pulsos V.

Para números impares: 00V

Para números pares: B0V

3.4.9 Objetivos de los códigos de línea

Eficiencia espectral. Se desea que el código de línea:

No presente componente continua. No contribuye al traspaso de información y genera dificultades en la recepción.

Presente pocas componentes espectrales de frecuencias cercanas a 0 Hertz. Con el objetivo de eliminar variaciones muy lentas de la señal que también dificultan la recepción.

Presente el menor ancho de banda posible en banda base.

Que las componentes espectrales fuera de la banda principal sean muy poco significativas, de modo que si se usan para modular una portadora, no generen muchas señales espurias.

3.4.10 Sincronismo y transparencia.

Se desea que el código incorporé información de reloj en los datos, que permita al receptor sincronizarse para detectar claramente los límites de tiempo de cada símbolo recibido.

Que esta información no requiera de una señal especial, sino que sea parte de los datos, incorporando transiciones suficientes en ellos.

Que estas transiciones no impliquen un aumento de ancho de banda

Que la información de sincronismo pueda recuperarse sin importar el número de ceros o de unos sucesivos que vayan en la información.

Capacidad de detección de errores. Se desea que el código:

Incorpore información codificada que permita que el receptor pueda detectar la aparición de errores en la recepción.

Ejemplos de códigos que permiten realizar la detección de errores por codificación de línea:

Código AMI, HDB3

Baja probabilidad de errores. Se desea que el código:

Presente cierta inmunidad al ruido, de modo que el receptor no incurra en muchos errores en la detección de los símbolos recibidos. Este parámetro se conoce como **BER:** Bit Error Rate o tasa de errores.

Dos décadas atrás, era normal considerar un BER=10^{-3}, actualmente son valores aceptables BER<10^{-7}. Esto ha sido posible gracias a la fibra óptica, al uso extensivo

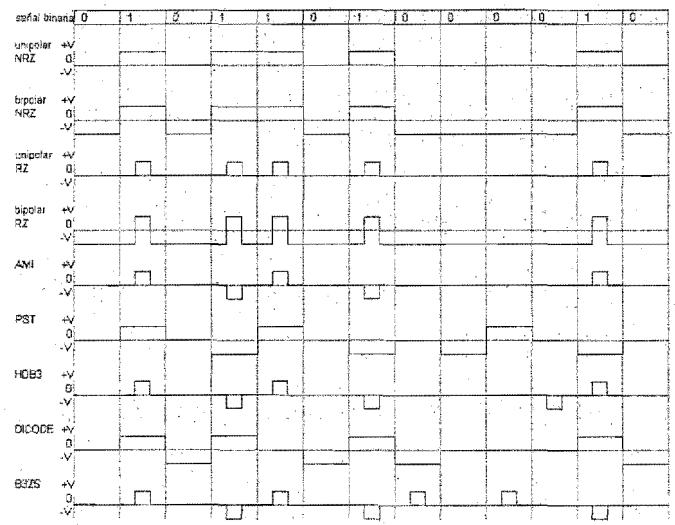


Figura 3.4.10-1 Códigos de línea

de códigos correctores de error en comunicaciones inalámbricas y a lazos de abonado más cortos en enlaces cableados.

Los códigos de línea adaptan la información digital en bits al canal de transmisión, para transmitir símbolos digitales.

3.5 Conversión analógica digital

Como una señal digital solo dispone de dos estados, esto es tiene un número finitos de niveles, se facilita la regeneración de la señal original sin perdida de la información u otros inconvenientes como diafonía, distorsión, etc. Los cuales son muy comunes en la transmisión de señal.

3.5.1 Característica de una señal

Cualquiera que sea el tipo de señal, analógica o digital, estas tienen parámetros que las caracterizan y que las hacen únicas, estas son:

Frecuencia (f): Es el numero de veces que se repite un ciclo de una señal por unidad de tiempo, las unidades de medición son los Hertz (hz.) equivalente a segundos Inversos (1/s).

Periodo (T): es la duración de un ciclo de una señal, cada cierto tiempo la señal se vuelve a repetir y es precisamente el tiempo que dura una repetición o ciclo. Las unidad de este parámetro son los segundos (s).

Fase (Θ): es la diferencia angular de adelanto a atraso de una señal con respecto a una referencia previamente establecida. Y sus unidades son los grados (Θ°).

Longitud de onda (λ): Es la distancia que recorre un ciclo de la señal.

Estos parámetros se relacionan con la señal con la siguiente formula:

$F(t) = A\text{sen}(wt + \Theta)$

Donde:

A = Amplitud pico o máxima de la señal, expresada en volts.

w = velocidad angular de la señal, expresada en grados.

$w = 2\pi f$

$\lambda = f/c$

f = frecuencia de la señal

c = velocidad de la luz (300 000 Km/s)

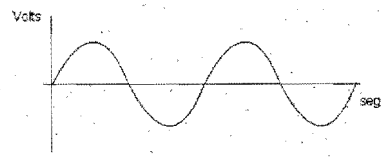


Figura 3.5.1-1 Señal analógica

3.5.2 Características de una señal analógica

Una señal es llamada analógica si al acotarla dentro de un intervalo de tiempo la amplitud toma un número infinito de valores. Como ejemplo una señal senoidal

3.5.3 Característica de la señal digital

Una señal es llamada digital si al acotarla dentro de un intervalo de tiempo, la señal toma un número finito de valores.

3.5.4 Ventajas y desventajas de las señales digitales

Las ventajas de las señales digitales sobre las analógicas son las siguientes:

Las señales digitales pueden soportar niveles más altos de distorsión e interferencia, se pueden regenerar sin que haya pérdida de la información. Son más seguras pues se pueden implementar códigos para detección y corrección de errores y su procesamiento es más sencillo. Las señales digitales pueden representar cualquier tipo de información: voz, datos y video.

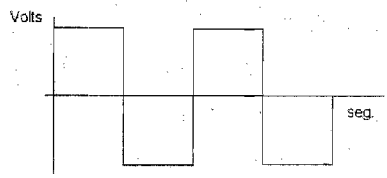


Figura 3.5.4-1 Señal digital

Al ocupar un mayor ancho de banda las señales digitales requieren ser transportadas en medios de transmisión más avanzados y por lo tanto más caros.

3.5.5 Conversión de la señal analógica a digital

La transformación de una señal analógica a digital se lleva a cabo en tres pasos básicos los cuales son:

Muestreo, cuantificación y codificación.

3.5.6 Muestreo

Para poder transferir el contenido de información de una señal no es necesario transmitir la señal completa, según el teorema de Nyquist y Shannon solo basta con enviar muestras discretas de la señal original tomadas al doble o mas de la frecuencia mas alta de esta.

$$F_s = 2f_{\max}$$

Ecuación 3.5.6-1 Frecuencia de muestreo

Para la voz, el ancho de banda es de 300 Hz. a 3.4 KHz. pero para su uso en el sistema telefónico el ancho de banda se extiende hasta los 4 Khz. por lo que la frecuencia de muestreo es: fs = (4000 Hz.) = 8000 Hz.

Si la frecuencia de muestreo es menor ala frecuencia máxima de la señal, la reconstrucción de la señal será imposible y esta tendrá errores.

3.5.7 Cuantificación.

La cuantificación nos permite representar la amplitud de una muestra con la amplitud del nivel discreto más cercano, esto significa que el valor real muestreado será representado por un valor cercano pero no igual.

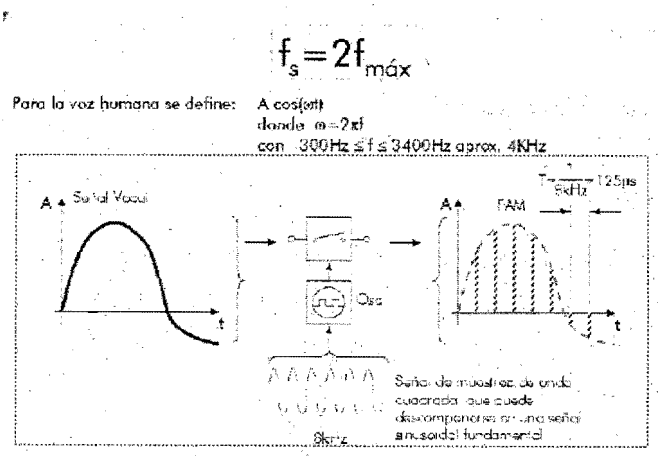


Figura 3.5.7-1 Muestreo de una señal

Los valores discretos permitidos son únicos y los valores entre estos valores discretos no pueden ser representados. Cada valor de la muestra tendrá que ser representado por un código. Dado que el número de códigos es limitado, los valores de la magnitud serán redondeados al valor más cercano.

El numero de niveles de cuantificación "M" esta estrechamente relacionado con el numero de bits "n" que son necesarios para codificar una señal. Para el caso del sistema telefónico, sea el sistema americano o el europeo, se usan 8 bits para codificar cada muestra, por lo tanto:

$M = 2^8 = 256$ niveles de cuantificación

Hay dos métodos principales para cuantificación de una señal: cuantificación lineal y cuantificación no lineal.

3.5.8 Cuantificación lineal

El rango total de valores de voltaje que pueden ser manejados es subdividido en un número de sub-rangos de voltaje iguales. Cada sub-rango corresponde a una combinación de código. Para cualquier valor dentro del un sub-rango, ya sea un valor en el limite inferior del sub-rango, o un valor en el limite superior del sub-rango, ambos serán codificados con el mismo código.

En el momento de decodificar, un código es representado por un voltaje correspondiente a la mitad del sub-rango (nivel de cuantificación).

El resultado es que cierta cantidad de ruido es adicionada a la señal original, esto es llamado ruido de cuantificación.

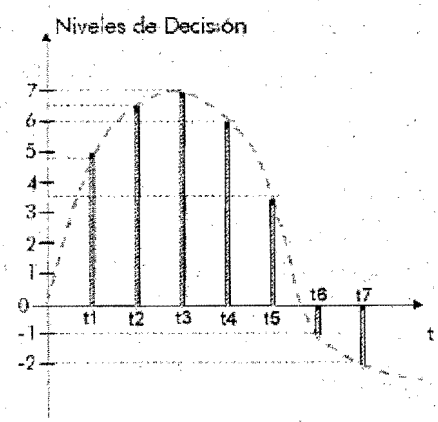


Figura 3.5.8-1 Cuantificación de una señal

El ruido de cuantificación es la diferencia entre la señal codificada cuantificada y la señal original. Este ruido, en el caso de cuantificación lineal, tiene un cierto nivel, dependiendo de los sub-rangos. Como resultado de la cuantificación lineal, se tiene el mismo ruido insertado tanto para pequeños valores como para altos valores de entrada. Esto significa que el ruido insertado para señales de valores pequeños tendrá relativamente mucha mas importancia que el ruido insertado en las señales de valores altos. La relación señal a ruido (SNR) será peor para las señales pequeñas.

3.5.9 Cuantificación no lineal

Como la cuantificación lineal de señales resulta en una mala relación señal a ruido, se utiliza otra clase de cuantificación con un valor constante de la señal a ruido, para cualquier nivel de la señal. Los niveles de cuantificación tienen que ser seleccionados de un modo logarítmico. Esto significa que se usara una cuantificación no lineal.

Las curvas logarítmicas tienen la desventaja, de que no pasan por el origen.

Hay dos leyes para resolver este problema:

3.5.10 Curva de la ley A

La curva de la ley A es estandarizada por CEPT y UIT-T usado en Europa, también conocida como de 13 segmentos.

Se utiliza la línea tangente a la curva desde el origen hasta los puntos de tangencia.

3.5.11 Curva de la ley μ

La curva de la ley μ es estandarizada por la North American Bell y UIT-T, obtiene una curva a través del origen al desplazar toda la curva al origen.

3.5.12 Codificación

Después de ser cuantificada, la muestra de entrada, esta limitada a 256 valores discretos. La mitad de estos son muestras codificadas positivas y la otra mitad son muestras codificadas negativas. Existen muchos códigos diferentes, pero los códigos más usados son: código natural y código simétrico.

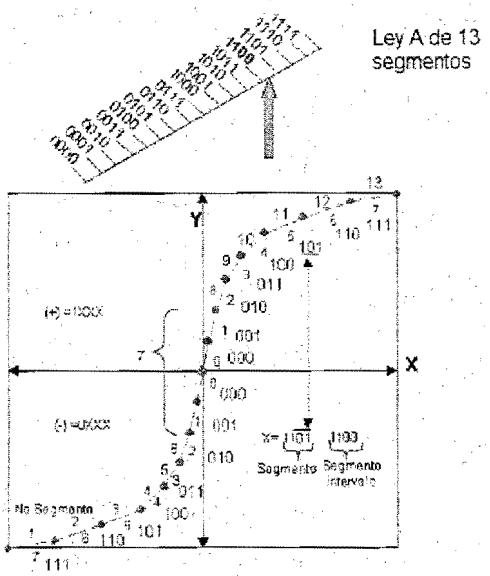


Figura 3.5.12-1 Curva de la Ley A

3.5.13 Código natural

Usando el código natural, el nivel de señal mas bajo (valor más negativo) corresponderá al código con el peso menor (00000000) y el valor más alto de la señal (valor más positivo) corresponderán al código con el peso más alto (11111111).

3.5.14 Código simétrico

En este código, los 8 bits están divididos en dos partes:

1 bit de signo y 7 bits de magnitud. El primer bit (bit de signo) corresponde al signo de la señal. Cuando el bit de signo es 1, se tiene un valor positivo, cuando el bit es 0, se tiene un valor negativo. Este código es el normalmente usado.

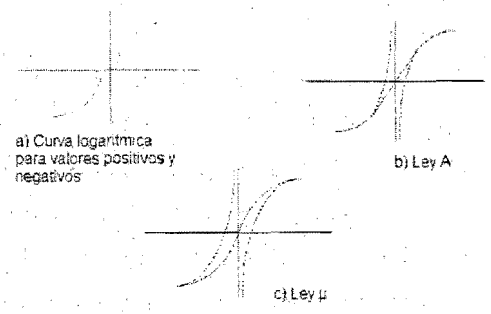


Figura 3.5.14-1 Curvas de la ley A y ley u

La ley A se divide en 13 segmentos. En la mitad inferior caen las muestras con polaridad negativa y en la mitad superior, las positivas. Cada segmento contiene 16 niveles, excepto el nivel 7 que tiene 64 niveles (realmente son cuatro niveles en uno). Sumando todos los niveles obtenemos 256 niveles de cuantificación, que son los empleados por esta ley.

3.6 Protocolo TCP/IP

El conjunto de protocolos asociados a TCP/IP es ampliamente utilizado en redes empresariales así como en el Internet el protocolo IP es un protocolo de red mientras que el protocolo TCP es un protocolo de transporte, sin embargo ambos trabajan en conjunto, realizando sus tareas correspondientes en procesos de direccionamiento, ruteo y establecimiento de conexiones orientadas y no orientadas. El protocolo TCP/IP tiene los siguientes componentes principales: IP, TCP y UDP.

3.6.1 Protocolo IP

El protocolo IP es un protocolo de nivel de red que proporciona servicios son conexión sobre muchos protocolos de capaz superiores. IP no garantiza la entrega de datagramas, aunque hace el mejor esfuerzo posible para entregar los datos. Los protocolos de capas superiores como TCP pueden usarse para construir servicios con entregas garantizadas sobre IP. IP proporciona la noción de red lógica independiente del nivel subyacente. Hace uso del protocolo de resolución de direcciones (ARP) para proporcionar el enlace entre direcciones lógicas (las direcciones IP) y las direcciones físicas (MAC) de un nodo.

Los datagramas IP se pueden fragmentar en unidades más pequeñas para acomodarse a la unidad de transmisión máxima (MTU) de la red subyacente. La MTU es el tamaño máximo de datos para cada paquete que se puede enviar sobre un tipo de red. Por ejemplo las rede Ethernet tiene un tamaño máximo de MTU de 1500 bytes.

La fragmentación se lleva a cabo siempre que los datos al ser enviados exceden la MTU de la red subyacente. Si la fragmentación tiene lugar, los fragmentos se crean con suficiente información para poder ser reensamblados. El reensamblaje de fragmentos para construir el datagrama original se hace en el nodo destino. Los problemas con IP, como los destinos inalcanzables y las temporizaciones en reensamblaje, se comunican al servidor usando el protocolo de mensajes de control de Internet (ICMP).

Las direcciones IP se presentan mediante un número de 32 bits. Cada interfaz de red en un nodo que soporta la pila de protocolos IP debe tener una dirección IP única asignada. La dirección IP es una dirección en dos partes formada por un identificador de red (netid) y un identificador de host (hostid) como se muestra Figura 3.6.1-2 los bits mas significativos se usan para determinar cuantos bits se están usando para el netid y el hostid. Se han definido cinco clase de direcciones: A, B, C, D y E, de estas, las direcciones de las clases A, B y C son asignables. La clase D esta reservada para multi-difusión y se usa en protocolos especiales para transmitir mensajes a un grupo seleccionado de nodos. La clase E se reserva para un uso futuro.

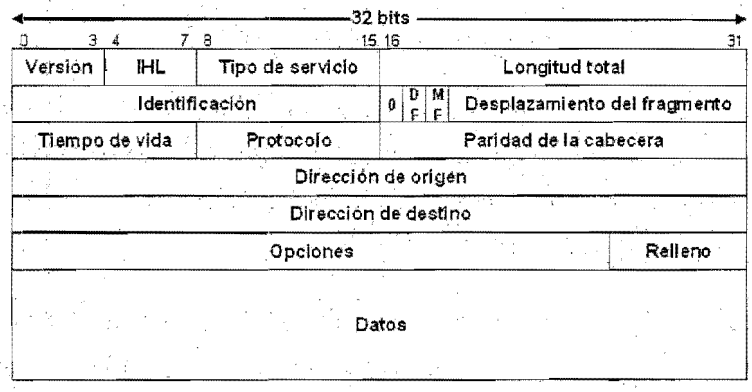


Figura 3.6.1-1 Encabezado IP

La porción netid de la dirección IP es similar al número de red usado en los protocolos IPX. Esta porción identifica la red de forma única. Todas las NIC en una subred deberán tener el mismo netid. Las redes interconectadas deben tener netid únicos.

Las redes de clase A son adecuadas para redes muy grandes, pero debido a que sus campos netid usan únicamente 7 bits, solamente pueden existir 127 redes. Las redes de clase B son redes de tamaño medio adecuadas para organizaciones de tamaño medio o grande. Las redes de clase C son adecuadas para organizar pequeñas, en las cuales cada red no puede tener más de 254 nodos.

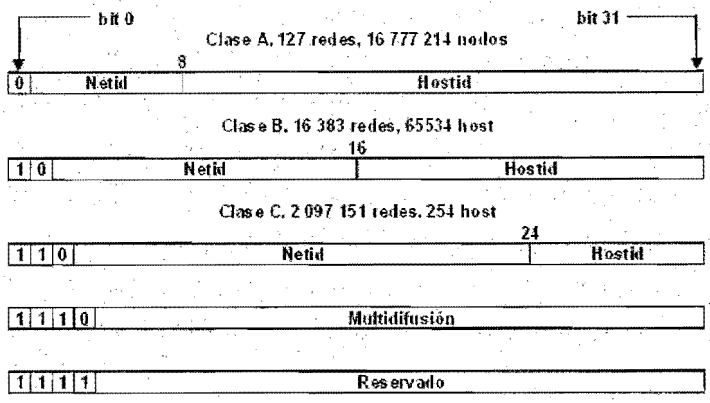


Figura 3.6.1-2 Clases de Direcciones IP

El número de 32 bits se representa por conveniencia como cuatro números decimales que se corresponden con el valor decimal de los cuatro bytes que forman la dirección IP de 32 bits. Los números decimales se separan por puntos, a esta notación se le llama notación decimal puntuada.

El campo versión es de cuatro bits de longitud e indica el formato de la cabecera IP. Esta característica permite que se puedan definir futuras estructuras de paquetes IP. El número de la versión actual es el cuatro, que indica IPV4.

La longitud de cabecera de Internet (IHL) es la longitud de la cabecera en palabras de 32 bits. Este campo es necesario porque la cabecera de IP contiene un campo opcional de longitud variable.

El tipo de servicio (ToS) informa a las redes de la calidad de servicio (QoS) deseada, la precedencia, retraso, rendimiento y fiabilidad.

El campo precedencia refleja el origen militar de las redes IP. La lista siguiente describe algunos valores de las precedencias:

Flash, tan pronto como sea posible; prioridad máxima en todos los circuitos

Inmediata, en cuatro horas

Prioridad, el mismo día

Rutina, un día.

La mayoría de las implementaciones IP y de los protocolos de enrutamiento (por ejemplo RIP) ignoran el campo ToS.

El campo precedencia se pensó para aplicaciones del departamento de defensa basadas en los protocolos de Internet. El uso de valores distintos a cero en este campo esta fuera del ámbito de la especificación estándar de IP.

Aunque se ha usado muy poco en el pasado, se espera que el papel del campo ToS se incremente muy pronto con protocolos de enrutamiento, como abrir la ruta de acceso mas corta primero (OSPF), que podrían usar el campo ToS. Se espera que se use para controlar dos aspectos de los protocolos de enrutamiento: algoritmos de enrutamiento y encolamiento. El campo ToS también se puede proyectar sobre el nivel de enlace para implementar compartir de manera efectiva de líneas series por diferentes clases de trafico TCP.

El campo longitud total contiene la longitud de la cabecera y de los datos IP en bytes. El tamaño máximo de datagrama es de 65 535 bytes. Todos los nodos IP deben estar preparados para recibir un mínimo tamaño de 576 bytes (512 bytes de datos mas 64 bytes de sobrecarga del protocolo).

El campo identificación se activa únicamente para cada datagrama y es el número de datagrama. Se usa con los modificadores No fragmentar (DF), Mas fragmentar (MF) y el campo desplazamiento de fragmento para reensamblar el datagrama. Si el modificador DF esta a 1, el datagrama no debería ser fragmentado. Un modificador MF a 1, indica al receptor que van a venir más fragmentos. Un MF a cero indica que este es el último fragmento.

El campo desplazamiento del fragmento indica la posición de los lados del fragmento relativos al principio del datagrama original. Este campo de 13 bits se mide en grupos de 8 bytes, lo que significa qué el valor del desplazamiento del fragmento debería ser multiplicado por 8 para obtener el desplazamiento en bytes.

El campo tiempo de vida (TTL) se mide en segundos y representa el tiempo máximo que un datagrama IP puede sobrevivir sobre la red. Debería decrementarse en cada ruteador con la cantidad de tiempo que ha llevado procesar el paquete. La intención es que la expiración de TTL origine que el datagrama sea descartado por un ruteador, pero no por el host de destino. El campo TTL tiene dos funciones: limitar el tiempo de vida de los segmentos TCP y terminar los bucles de enrutamiento en Internet. Aunque el campo TTL se especifica en segundos, también tiene algunos atributos relacionados con el contador de saltos debido a que cada ruteador tiene que reducir el campo TTL con el numero de segundos que el ruteador mantiene el paquete o por lo menos en 1 segundo.

El campo protocolo indica que protocolo de nivel superior va a recibir los datos IP. TCP por ejemplo, tiene un campo de protocolo con un valor de 6, UDP tiene un valor de 17.

La paridad de la cabecera se usa solamente para la cabecera IP. Para calcularla se complementa 1 bit de cada 16 bits que componen la cabecera (excluyendo el campo paridad de la cabecera).

Luego se calcula el complemento a 1 de la trama. Este campo es recalculado en cada ruteador debido a que el valor de campo TTL es disminuido y por lo tanto se modifica la cabecera.

Las direcciones de origen y de destino son las direcciones IP de 32 bits que los nodos de origen y de destino.

3.6.2 Protocolo TCP

TCP es el protocolo de transporte primario que se usa para proporcionar conexiones con circuitos virtuales fiables, Full duplex y orientados a flujo. Las conexiones con circuitos virtuales se establecen entre los números de puertos de los nodos receptores y transmisores. Los datos se pueden enviar a través de un circuito virtual simultáneamente en ambas direcciones, lo que hace que los circuitos virtuales sean full- duplex. El protocolo TCP es orientado a flujo y tiene en cuenta el número de octetos en cada dirección. No existe limitaciones en el numero de conexiones de circuitos virtuales entre dos hosts TCP excepto entre aquellas relacionadas con la memoria necesaria para mantener las tablas de estado para las conexiones y los host TCP. La Figura 3.6.2-1 muestra la estructura de paquetes TCP. Los números de puertos origen y destino identifican los procesos de los extremos en el circuito virtual de TCP. Los números de puertos del 0 al 1024 se asignan a servicios predeterminados por el sistema. El número de secuencia de 32 bits indica el número del byte de datos en el mensaje actual. Si el modificador SYN esta en 1, este campo define el numero de secuencia inicial para usar en esa sección. Se usa un valor de 32 bits para evitar el uso de números de secuencia antiguos que podrían ya haber sido asignados a datos en transito por la red. El número de confirmación indica el número de secuencia del siguiente byte esperado por el receptor. Las confirmaciones de TCP son acumulativas, es decir, una sola confirmación se puede usar para confirmar cierto número de segmentos de mensajes anteriores de TCP. El campo desplazamiento de datos es el numero de palabras de 32 bits en la cabecera TCP. Este campo es necesario por que el campo opciones de TCP puede variar en longitud.

El modificador URG se usa para evitar datos fuera de banda sin esperar a que el receptor procese los octetos que ya están en flujo. Cuando el modificador URG esta activo, el campo posición urgente es valido. Una implementación de TCP debe soportar una secuencia de datos urgentes de cualquier longitud. Aunque el mecanismo de urgente puede ser usado por cualquier aplicación, se usa normalmente para enviar comandos de tipo interrupción a un programa Telnet.

El modificador ACK indica que el campo numero de confirmación es valido.

El modificador PSH le dice a TCP que entregue inmediatamente los datos para este mensaje al proceso de nivel superior.

El bit RST se emplea en un circuito virtual debido a errores irrecuperables. La razón podría ser una caída del host o paquetes SYN duplicados y retrasados.

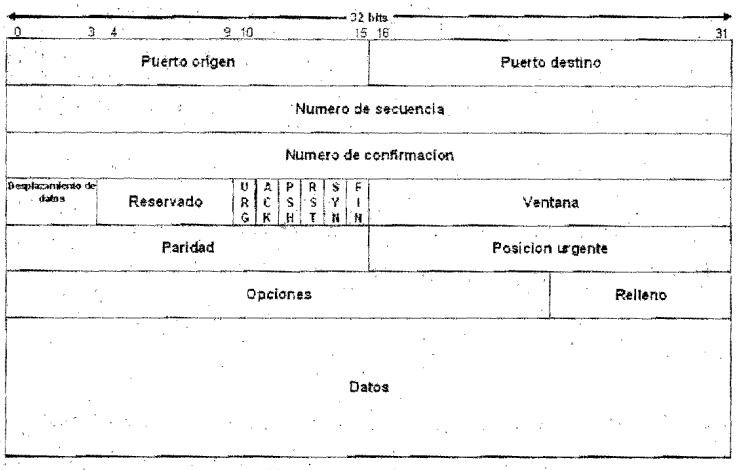


Figura 3.6.2-1 Encabezado TCP

El modificador SYN indica I apertura de una conexión en un circuito virtual. Las conexiones TCP se abren usando un procedimiento de saludo en tres partes. Los modificadores YN y ACK se usan para indicar estos paquetes:

SYN = 1 y ACK = 0	Paquete de abrir conexiones
SYN = 1 y ACK = 1	Confirmación de conexión abierta
SYN = 0 y ACK = 1	Paquete de datos o paquete de ACK

El modificador FIN termina la conexión. La terminación de una conexión en TCP se lleva a cabo con un mecanismo de cierre acordado: ambos lados deben de estar de acuerdo en términos enviándose un modificador FIN = 1 antes de que la terminación de la conexión pueda ocurrir. Este cierre acordado asegura que no hay pérdida inesperada de datos en cualquiera de los lados debido a un corte abrupto de la conexión.

El campo ventana sirve para implementar el control de flujo y lo usa el receptor para anunciar el número de bytes adicionales de datos que quiere aceptar.

El campo paridad es el complemento a 1 de la suma de todas las palabras de 16 bits en el paquete TCP. Una seudo-cabecera de 96 bits es preañadida a la cabecera de TCP para la computación de la paridad. La seudo-cabecera identifica si el paquete ha llegado al destino adecuado.

El campo opciones define la opción tamaño de segmento máximo (MSS), que se negocia durante el establecimiento de la conexión.

3.6.3 El protocolo UDP

A diferencia de TCP que esta orientado a conexión, UDP opera en modo datagrama. UDP no hace ningún intento de crear una conexión. Los datos se envían encapsulándolos en una cabecera UDP y pasándolos al nivel de IP. El nivel de IP envía el paquete UDP en un único datagrama IP a menos que se requiera la fragmentación. UDP no intenta proporcionar secuenciamiento de los datos. UDP es útil en aplicaciones de tipo petición/respuesta y donde las peticiones y las respuestas se pueden enviar en un único datagrama. No existe la sobrecarga de abrir y cerrar la conexión para enviar una pequeña cantidad de datos. Otra ventaja de UDP es su uso en aplicaciones que requieren difusión / multi-difusión. El nivel de red subyacente podría usar sus capacidades de difusión / multi-difusión para enviar los datos.

El campo puerto origen es un campo opcional de 16 bits, cuando tiene sentido indica:

El numero de puerto del proceso que envía

El número de puerto del origen es el puerto al cual debería enviarse la respuesta en ausencia de cualquier otra información.

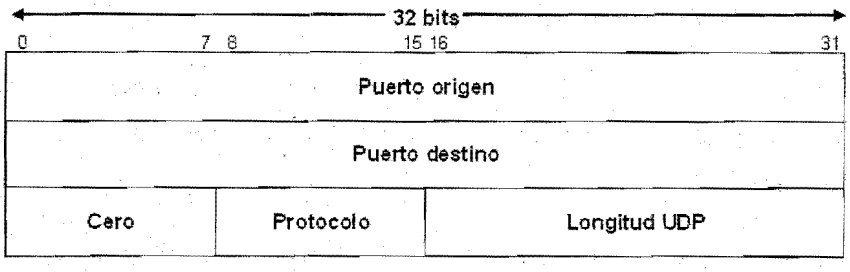


Figura 3.6.3-1 Encabezado UDP

El campo puerto destino identifica el proceso en la dirección IP destino que va a recibir los datos UDP que se han sido enviados.

El campo longitud es la longitud del paquete UDP en octetos. Esta longitud incluye la cabecera UDP y sus datos.

El campo paridad es el complemento a 1 en 16 bits de la suma de los complementos a 1 de la pseudo-cabecera de información de la cabecera IP.

3.7 Redes LAN

Una red LAN es una red de datos de alta velocidad, tolerante a fallas que cubren un área geográfica relativamente pequeña. Por lo general conecta a estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. Las LAN permiten a los usuarios intercambiar información, compartir dispositivos y aplicaciones entre varios usuarios y la comunicación de los usuarios vía correo electrónico o Chat.

Los protocolos LAN operan en las dos capas mas bajas del modelo de referencia OSI, entre las capas físicas y la capa de enlace de datos.

3.7.1 Métodos de acceso al medio de LAN

Los protocolos LAN suelen utilizar dos métodos para acceder el medio físico de la red: CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones) y estafeta circulante.

En el esquema de acceso a medios CSMA/CD, los dispositivos de la red compiten por el uso del medio de transmisión físico de la red. Ejemplos de LAN que utilizan el acceso a medios CSMA/CD son las redes Ethernet/IEEE 802.3, incluyendo a 100BaseT.

En el esquema de acceso a medios llamado estafeta circulante, los dispositivos de la red accedan al medio de transmisión con base en la posesión de una estafeta. Ejemplos de esto son las redes Token Ring/IEEE 802.5 y FDDI.

Los métodos de transmisión en las redes LAN caen dentro de tres clasificaciones:

Uni-difusión

Multi-difusión

Difusión

En las transmisiones de uni-difusión, sé envía un solo paquete desde el origen hacia un destino de la red. Primero el nodo origen direcciona el paquete utilizando la dirección del nodo destino, luego el paquete es enviado por la red y finalmente, la red transfiere el paquete a su destino.

La transmisión de multi-difusión consta de un solo paquete de datos que se copia y envía a un subconjunto específico de nodos de red. Primero el nodo origen direcciona el paquete utilizando una dirección de multi-difusión. Luego, el paquete es enviado a través de la red, la cual genera copias del paquete y envía estas copias a cada uno de los nodos que se indican en la dirección de multi-difusión.

La transmisión de difusión consta de un paquete de datos que se copia y envía a todos los nodos de la red. En este tipo de transmisión, el nodo origen dirige el paquete utilizando la dirección de difusión. El paquete es, luego enviado a través de la red, la cual hace copias del paquete y las envía a cada uno de los nodos de la red.

3.7.2 Topologías de redes LAN

Las topologías definen la forma en que están organizados los dispositivos de la red. Hay cuatro topologías comunes de LAN: bus, anillo, estrella y árbol o jerárquica. Estas topologías son arquitecturas lógicas, sin embargo los dispositivos en realidad no necesitan estar ubicados físicamente de acuerdo con estar configuraciones.

3.7.3 Dispositivos de redes LAN

Los dispositivos mas comunes de una red LAN son repetidores, concentradores o hub, switches y ruteadores. Un repetidor es un dispositivo de la capa física que se utiliza para interconectar los segmentos de cable en una red extendida. En esencia, un repetidor hace posible que una serie de segmentos de cable se comporte como un solo cable. Los repetidores reciben señales de un segmento de sed y amplifican, re-sincronizan y retransmiten esas señales hacia otro segmento de la red. Un concentrador o hub es un dispositivo de capa física que conecta varias estaciones de usuario por medio de un cable dedicado. Las interconexiones eléctricas se establecen dentro del concentrador. Los concentradores se utilizan para conformar una red con topología física en estrella que a su vez conserva la topología lógica en bus o la configuración en anillo de LAN. En algunos aspectos, el concentrador actúa como repetidor multipuesto. Los switches son dispositivos de capa 2 que actualmente están sustituyendo a los hub debido a que incrementan la optimización del canal de comunicación entre estaciones que se comunican. El ancho de banda ya no es compartido por todas las estaciones conectadas al dispositivo switch y entre cada una puede haber incluso un canal de comunicación full duplex 100 Mbps. Reduciendo el trafico. Algunos switch que tienen la capacidad de ser administrados, permiten realizar VLAN entre las computadoras de la red. Los ruteadores son

dispositivos de capa 3 que se encargan del ruteo de los paquetes entre redes de diferentes segmentos, algunos dispositivos cuentan con características avanzadas como un firewall integrado en el mismo dispositivo e incluso un punto de acceso. Algunos ruteadores son usados como gateway hacia el Internet.

3.7.4 Tecnologías Ethernet

El término ethernet se refiere a la familia de implementaciones de LAN que incluyen las tres categorías principales:

Ethernet e IEEE 802.3, son las especificaciones LAN que operan a 10 Mbps a través de cable coaxial y cable de par trenzado

Ethernet a 100 Mbps, es una especificación LAN, también conocida como Fast ethernet, que opera a 100 Mbps a través de cable de par trenzado o fibra óptica.

Ethernet a 1000 Mbps, es una especificación LAN también conocida como Gigabit ethernet, que opera a 1000 Mbps a través de fibra óptica y de par trenzado.

Los estándares LAN especifican el cableado y señalización de las capas físicas y de enlace de datos del modelo OSI.

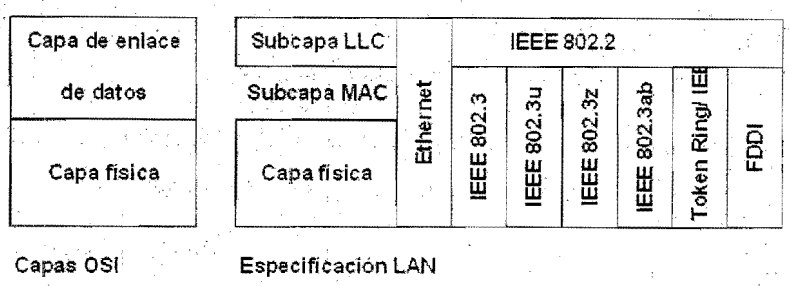


Figura 3.7.4-1 Especificaciones Ethernet

El estándar ethernet esta basado en el acceso múltiple por detección de portadora/detección de colisiones (CSMA/CD) y es especificado en la capa física y el la sub-capa de control de acceso al medio de la capa de enlace de datos.

La IEEE dividió la capa de enlace de datos en dos sub-capas separadas:

LLC, control de enlace lógico (transmisión hacia las capas superiores de la red)

MAC, control de acceso al medio (transmisión hacia debajo de la capa física).

El IEEE creo la sub-capa LLC para permitir a la capa de enlace de datos funcionar independientemente de las tecnologías existentes. Esta capa proporciona versatilidad en servicios de protocolos de capa de red que están arriba de ella, mientras se comunica efectivamente con la MAC y una variedad de tecnologías de capa física. La sub-capa LLC participa en el proceso de encapsulamiento.

La sub-capa MAC negocia con el acceso al medio físico. La especificación MAC de la IEEE define una dirección MAC, que identifica de manera única a los dispositivos en la capa de enlace de datos. Cada dispositivo debe tener una dirección MAC única para poder participar en la red.

Hay cuatro protocolos comunes relacionados a Ethernet. Ethernet se refiere a la familia de protocolos LAN y estos incluyen cuatro implementaciones populares:

1. 10 Mbps Ethernet: esta especificación LAN (IEEE 802.3 y Ethernet II) opera a 10 Mbps sobre cable coaxial y cable de par trenzado

2. 100 Mbps Ethernet: esta especificación LAN (IEEE 802.3u) también conocida como Fast Ethernet, opera a 100 Mbps sobre cable de par trenzado.

3. Gigabit Ethernet: es una extensión del estándar Ethernet 802.3, gigabit Ethernet incrementa la velocidad de fast Ethernet hasta 1000 Mbps. Estos dos estándares IEEE 802.3z (estándar para operación a 1000 Mbps sobre fibra óptica) y 802.3ab (estándar para operación a 1000 Mbps sobre UTP) definen la operación de gigabit Ethernet sobre fibra coaxial y cable de par trenzado.

4. 10000 Mbps Ethernet: esta versión podría ser implementada en el futuro cercano.

La descripción de protocolo ethernet es como sigue:

El primer número indica la velocidad de la red LAN en Mbps.

El termino BASE se refiere a que es una señal en banda base, la otra opción seria banda ancha.

El tercer término indica el tipo de cable y la longitud máxima, si hay número la longitud máxima es el valor del número multiplicado por 100 y expresado en metros.

3.8 Redes WAN

Una de WAN es una red de comunicación de datos que tiene una cobertura geográfica relativamente grande y suele utilizar las instalaciones de transmisión que ofrecen compañías portadoras de servicio como los operadores telefónicos. Las tecnologías WAN operan en las tres capas inferiores del modelo de referencia OSI: La capa física, la capa de enlace de datos, y la capa de red.

3.8.1 Circuitos conmutados

Este método de acceso da a cada usuario una ruta dedicada hacia la red. Para que pueda operar se tiene que establecer un proceso de marcación, también llamado señalización. La configuración de la llamada un canal separado no usado por el trafico de datos. El mas comúnmente usado es la señalización de sistema siete (SS7) la cual usa mensajes de control de llamada y señalización entre los punto de transferencia.

Figura 3.8.1-1 Red WAN punto-punto

3.8.2 Multiplexión por división de tiempo (TDM)

Los datos de varios orígenes tienen una asignación de ancho de banda en un medio único. Los circuitos conmutados usan la señalización para determinar la ruta de la llamada, que es una ruta dedicada entre el que envía y el que recibe. A través de la multiplexión del tráfico en ranuras de tiempo fijas, TDM evita congestión y retardos. Los servicios básicos de telefonía e ISDN usan circuitos TDM.

3.8.3 Frame Relay

La información contenida en frames comparte el ancho de banda con otros suscriptores WAN de Frame Relay. Frame Relay es un servicio de multiplexión estadístico. Distinto a TDM, frame Relay usa la capa 2 para identificar y mantener circuitos virtuales.

3.8.4 Enlaces punto a punto

Un enlace punto a punto proporciona una sola trayectoria de comunicación WAN preestablecida desde las instalaciones del cliente, a través de una red de transporte, propiedad de un operador telefónico, y hacia una red remota. A los enlaces punto a punto también se les conoce como líneas privadas, puesto que su trayectoria establecida es permanente y esta fijada de acuerdo a los requerimientos exclusivos del cliente que las contrata.

3.8.5 Conmutación de circuitos

La conmutación de circuitos es un método de conmutación WAN en la que se establece, mantiene y termina un circuito físico dedicado a través de una red de transporte para cada sesión de comunicación. La conmutación de circuitos maneja dos tipos de transmisiones: transmisiones de datagrama, que están compuestas de tramas direccionadas de manera individual y transmisiones en ráfagas de datos, que están compuestas de una ráfaga de datos para las que la verificación de direcciones solo se presenta una vez. La conmutación de circuito opera de manera muy parecida a una llamada telefónica.

3.8.6 Conmutación de paquetes

Este es un método de conmutación WAN en el que los dispositivos de la red comparten un solo enlace punto a punto para transferir los paquetes desde un origen hasta un destino a través de una red de transporte. El múltiplexaje estadísticos se utiliza para permitir que los dispositivos compartan estos circuitos. ATM (Modo de Transferencia Asíncrona), Frame Relay, y X.25, son ejemplos de tecnologías WAN de conmutación de paquetes.

3.8.7 Circuitos virtuales

Un circuito virtual es un circuito lógico creado para asegurar una comunicación confiable entre dos dispositivos de red. Hay dos tipos de circuitos virtuales: SVCs (Circuito Virtual Conmutado) y PVCs (Circuitos Virtuales Permanentes)

Los SVC son circuitos virtuales que se establecen dinámicamente por demanda y se terminan al finalizar la transmisión. La comunicación a través de un SVC tiene tres fases:

El establecimiento del circuito

La transferencia de datos

La terminación del circuito

La fase de establecimiento implica la creación de un circuito virtual entre los dispositivos origen y destino. La transferencia de datos implica la transmisión de datos entre los dispositivos a través de circuitos virtuales, y la terminación del circuito implica la desconexión del circuito virtual entre los dispositivos origen y destino. Los SVC se utilizan en situaciones donde la transmisión de datos entre los dispositivos es esporádica.

Un PVC es un circuito virtual que se establece de manera permanente y consta de un solo modo: Transferencia de datos

Los PVC se utilizan en situaciones donde la transferencia de datos entre los dispositivos es constante y/o se requiere una rápida respuesta. El costo de un PVC es muy superior a un SVC debido a su alta disponibilidad en cualquier momento (no requiere de establecer y terminar un circuito).

3.8.8 Dispositivos WAN

Las WAN utilizan distintos tipos de dispositivos como:

Router, que ofrecen muchos servicios, incluyendo puertos de interfaz WAN y LAN.

Switches WAN, tales como un switch ATM, usado para comunicación de voz datos y video.

MODEM y unidades de servicios de canal/ unidades de servicios de datos (CSU/DSU), las cuales son usadas como interfaces entre el dispositivo de usuario final (tales como computadoras o ruteadores) y el switch que proporciona el servicio.

Servidores de acceso, los cuales son usados para concentrar conexiones de módems, por ejemplo un ISP necesita un servidor de acceso para que los usuarios puedan llamar y autenticarse en la red antes de tener acceso a la red.

Los ruteadores son dispositivos que implementan los servicios de la capa de red, ellos proporcionan un amplio rango de interfaces, tales como ethernet, Fast ethernet y Gigabit ethernet para conexiones LAN y conexiones seriales y de ATM para WAN.

El Internet contiene muchos cientos de ruteadores, estos actúan como los policías de tráfico en el Internet que dirigen como un paquete debería de viajar para buscar su destino.

Los switch WAN es un dispositivo de red multi-puerto que conmuta el tráfico tales como Frame Relay, X.25 y ATM. Los switches WAN usualmente operan en la capa de enlace de datos del modelo de referencia OSI.

Los MODEM son dispositivos que interpretan señales digitales y analógicas a través de la modulación y de-modulación de señal, permitiendo a los datos ser transmitidos sobre líneas telefónicas de voz. En la fuente las señales digitales son convertidas en una forma que son convenientes para la transmisión sobre las facilidades de las

comunicaciones analógicas. En el destino, estas señales analógicas son regresadas a la forma digital para extraer la información que esta señal contenga.

Un CSU /DSU es un dispositivo de interfaz digital, que adapta la interfaz física en dispositivo de equipamiento de terminal de datos (DTE), tales como un computadora, a un dispositivo de equipamiento de terminación de circuito de dato (DCE), tales como un switch en una red de transporte conmutada. Algunas veces los CSU/DSU son integrados en las interfaces del ruteador.

Los enlaces WAN pueden ser ordenados a los proveedores de servicios en varias velocidades, las cuales son establecidas en bps (bits por segundo) estos bps determinan la capacidad de que tan rápidos pueden ser movidos a través de los enlaces WAN. Los más comunes son:

DSO = 64 Kbps

E1 = 2.048 Mbps estándar europeo de PDH

E3 = 34. 064 Mbps estándar europeo de PDH

T1 = 1.544 Mbps estándar americano de PDH

STM-1 = 155.52 Mbps estándar europeo para SDH

OC-1 = 51.840 Mbps estándar americano para SONET

OC-3 = 155.52 Mbps estándar americano para SONET

Los protocolos de capa física de las WAN describen como proporcionar conexiones eléctricas, mecánicas, operacionales y funcionales. La mayoría de las WAN requieren una interconexión que es proporcionada por el proveedor de servicios de comunicaciones. La capa física de la WAN también describe la interfaz entre el DTE

y el DCE. Típicamente el DCE es de el proveedor de servicios y el DTE es el dispositivo acoplado a el. Algunos de los estándares de capa física que conectan un DTE con DCE son entre otros:

EIA/TIA 232, soporta señales de 64 Kbps y es más conocida como RS-232

EIA/TIA-449, soporta señales de hasta 2Mbps.

EIA/TIA-612/613, este estándar describe la interfaz serial de alta velocidad (HSSI), la cual proporcionan servicio a T3, E3 y STS-1 de SONET. La velocidad depende de la interfaz del DSU y del tipo de servicio que es conectado.

G.703, esta especificación eléctrica y mecánica de la ITU-T para conexiones entre equipamiento de la compañía de teléfonos y un DTE usa conectores BNC y opera en las velocidades de un E1.

Los protocolos de la capa de enlace de datos describen como los frame son transportados en un enlace de datos. Estos están diseñados para operar sobre punto a punto, multipunto y servicios multi-acceso conmutado como Frame Relay. El encapsulamiento de la capa de enlace de datos asociado con las líneas seriales sincronías incluyen los siguientes:

HDLC, control de enlace de alto nivel (high level data link)

Protocolo de punto à punto (PPP), este protocolo contiene un campo de protocolo para identificar el protocolo de la capa de red que esta siendo transportado en el frame de PPP.

SDLC, control de enlace de datos sincrono (synchronous data link control), este protocolo es un diseño de IBM de protocolo de enlace de datos WAN para ambiente de arquitectura de redes de sistemas (SNA), esta siendo remplazado por HDLC.

LAPB (link access procedure, balanced), este protocolo de enlace de datos WAN es usado por X.25 y ISDN

LAPF (procedimiento de acceso al enlace para Frame Relay), este protocolo especifica la estructura de los frame, formato de los campos y procedimientos de acceso, es usado con las tecnologías de Frame Relay.

Las tecnologías de WAN para interconectar dos o mas redes LAN podrían ser entre otras: X.25, Frame Relay, DLS e ISDN.

Capitulo 4 Redes 802.11

4.1 Arquitectura de red 802.11

Cuando instalamos, configuramos y finalmente inicializamos un cliente Wireless LAN, tales como dispositivos USB, PCI o PCMCIA inalámbricos, el cliente automáticamente escuchara para ver si hay una LAN inalámbrica dentro del rango. El cliente es también descubierto si puede asociarse con la LAN inalámbrica. Este proceso de escuchar es llamado "escaneando" (scanning). Escaneando ocurre antes que cualquier otro proceso, puesto que al estar escaneando es la forma como el cliente busca la red.

Hay dos clases de búsquedas de puntos de acceso por parte de los clientes inalámbricos, búsqueda pasiva y búsqueda activa. En la búsqueda de un punto de acceso, las estaciones cliente siguen un rastro de migajas dejado por el punto de acceso. Estas migajas son llamadas "identificador del conjunto de servicio" (SSID) y señales guías (beacons). Estas herramientas sirven como un medio para que la estación cliente busque cualquier punto de acceso.

4.1.1 SSID

El identificador de conjunto de servicio (SSID) es único, sensitivo a valores alfanuméricos de 2 a 32 caracteres de longitud usado por las LAN inalámbricas como nombre de la red. Este manejo de nombres es usado para segmentar redes, como una rudimentaria medida de seguridad en el proceso de unirse a una red.

El valor del SSID en enviado en señales guía (beacons), requerimientos de prueba, respuestas de prueba y otro tipo de frames. Una estación cliente deberá ser configurada con el correcto valor de SSID a fin de unirse a la red. Este valore se configura en cada uno de los puntos de acceso y debe ser diferente en cada uno a fin de determinar a cual red sé esta conectando. Algunos clientes tienen la habilidad de usar cualquier valor de SSID a diferencia de solo uno especificado manualmente por el administrador. Si un cliente intenta hacer Roaming entre un grupo de puntos de acceso, el cliente y todos los puntos de acceso deben ser configurados con los

SSID de acoplamiento. El punto más importante sobre un SSID, es que debe acoplarse exactamente entre el punto de acceso y los clientes. No debe confundirse el SSID con el BSSID. El identificador de conjunto de servicios básicos (BSSID) es un número hexadecimal de 6 bytes que identifica al punto de acceso de donde el frame fue originado o fue relevado.

4.1.2 Señales guía (Beacons)

Las señales guías, son frames cortos que son enviados desde un punto de acceso a una estación (en el modo de infraestructura) o estaciona estación (modo ad-hoc) en orden para la sincronizar y organizar las comunicaciones inalámbricas en una LAN inalámbrica. Las señales guías sirve para algunas funciones incluyen las siguientes.

4.1.3 Sincronización de tiempo

Las señales guía (beacons) sincronizan a los clientes por medio de una marca de tiempo en un momento exacto de la transmisión. Cuando el cliente recibe la señal guía (beacon) el cambio su propio reloj para reflejar el reloj del punto de acceso. Una vez que este cambio ha sido hecho, los dos relojes están sincronizados. Sincronizando los relojes de las unidades de comunicación se asegura que todas las funciones sensitivas al tiempo, tales como saltos en sistemas FHSS, son desarrolladas sin errores. Las señales guías (beacons) también contienen el intervalo de las señales guía (beacon), que informa a las estaciones que tan frecuente puede esperar una señal guía (beacon).

4.1.4 Conjunto de parámetros FH o DS

Las señales guía (beacon) contienen información especifica adaptadas específicamente para las tecnologías de espectro disperso que el sistema esta usando. Por ejemplo, en un sistema FHSS, los parámetros de tiempo de salto de frecuencia y de tiempo de duración de la transmisión y secuencia de salto entre frecuencias son incluidos en las señales guía (beacon). En un sistema DSSS, los beacons contienen información del canal.

4.1.5 Información SSID

Las estaciones ven a las señales guía (beacon) por el SSID de la red a la cual ellas quieren unirse. Cuando esta información es encontrada, la estación ve la dirección MAC de donde se origino la señal guía (beacon) y envía un requerimiento de autenticación con la esperanza de asociarse con el punto de acceso. Si una estación es establecida para aceptar cualquier SSID, entonces la estación intentara unirse a la red a través del primer punto de acceso que envié su señal guía (beacon) o de uno con la señal mas fuerte si hay múltiples puntos de acceso.

4.1.6 Mapa de indicación de trafico (TIM)

El TIM es usado como un indicador de cual estación que esta durmiendo (sleeping), tienen paquetes están encolados en el punto de acceso. Esta información es pasada en cada señal guía (beacon) a cada estación asociada. Mientras "duermen", las estaciones sincronizadas, enciende sus receptores, escuchando las señales guía (beacon), revisan el TIM para ver si ellos (los paquetes encolados) están listos, entonces si ellos no están listos, la potencia baja en los receptores y continúan durmiendo.

4.1.7 Velocidades soportadas

Con redes inalámbricas, hay varias velocidades soportadas dependiendo del estándar del el hardware usado. Por ejemplo un dispositivo que cumple con el estándar 802.11b, soporta 11, 5.5, 2 y 1 Mbps de velocidad de transmisión. Esta información de capacidad es pasada en las señales guía (beacon) para informar a las estaciones que velocidades son soportadas por el punto de acceso.

4.1.8 Escaneo pasivo

Escaneo pasivo es el proceso de escuchar las señales guía (beacon) en cada canal por un periodo específico de tiempo después de que la estación es inicializada. Estas señales guía (beacon) son enviadas por puntos de acceso (en modo

infraestructura) o por estaciones cliente (en modo ad-hoc) y la estación que escanea, cataloga las características sobre el punto de acceso o estaciones basadas en estas señales guía (beacon). La estación que esta buscando una red, escucha a las señales guía (beacon) hasta que esta escucha una señal guía (beacon) que contenga el SSID de la red a la que se quiere unir. La estación entonces intenta unirse a la red a través del punto de acceso que envía la señal guía (beacon).

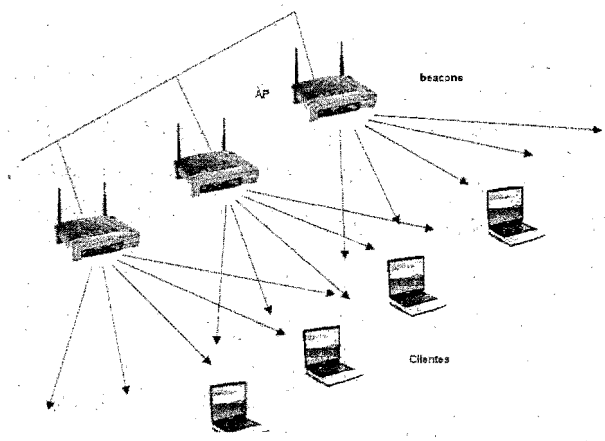


Figura 4.1.8-1 Escaneo pasivo

Las estaciones continúan escaneando pasivamente incluso después de la asociación con un punto de acceso. Escaneo pasivo ahora tiempo reconectando a la red, si el cliente es desconectado de un punto de acceso al cual el cliente este actualmente conectado.

A través de mantener una lista de puntos de acceso disponibles y sus características (canal, fuerza de la señal, SSID, etc.), la estación puede rápidamente localizar el mejor punto de acceso si su actual conexión se rompiera por alguna razón.

Las estaciones pueden hacer Roaming de un punto de acceso a otro, después de que la señal de radio del punto de acceso donde la estación esta conectada, toma

valores bajos. El Roaming es implementado para que las estaciones puedan mantenerse conectadas a la red. Las estaciones usan la información obtenida a través del escaneo pasivo para localizar el siguiente mejor punto de acceso, para usar para conectividad en la red. Por esta razón, él traslape entre células de puntos de acceso, es usualmente especificado en alrededor de 20 a 30 %. Este traslape permite a las estaciones hacer Roaming entre puntos de acceso mientras se conectan y desconectan sin que el usuario tenga conocimiento de esto.

4.1.9 Escaneo activo

El escaneo activo esta relacionado con el envío de un frame de requerimiento de prueba desde una estación inalámbrica. Las estaciones envían este frame de prueba cuando ellos están activamente buscando una red para unirse. Este frame de prueba contendrá un SSID de la red al cual desea unirse o un broadcast de SSID. Si el

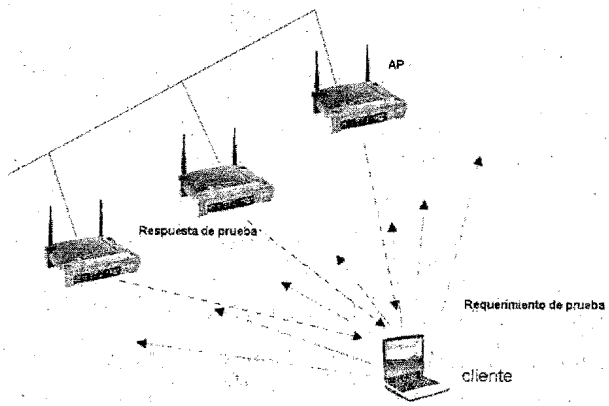


Figura 4.1.9-1 Escaneo activo

requerimiento de prueba es enviado especificando un SSID, entonces solo el punto de acceso que esta utilizando este SSID, responderá con una prueba de frame de respuesta. Si una prueba de frame de requerimiento es enviada con u broadcast de SSID, entonces todos los puntos de acceso dentro de la búsqueda responderán con una prueba de frame de respuesta.

Una vez que un punto de acceso con el apropiado SSID es encontrado, la estación inicializa los pasos la autenticación y la asociación para unir a la red a través del punto de acceso.

La información pasada de un punto de acceso a una estación en la prueba de frame de respuesta es en mayoría idéntica a las señales guía (beacon). Las pruebas de frame de respuesta difiere de las señales guía (beacon) solo en que no tiene marcas de tiempo y no incluyen el mapa indicador de trafico (TIM).

La fuerza de la señal de la prueba de frame de respuesta que la tarjeta de red inalámbrica recibe ayuda a determinar con que punto de acceso intentará asociarse. La estación generalmente seleccionara el punto de acceso con la señal más fuerte y razón de tasa de errores más baja (BER). El BER es la razón de los paquetes malos a los paquetes buenos, típicamente determinado por la relación señal a ruido de la señal. Si el pico de una señal de RF esta cercana al piso de ruido, entonces el receptor puede confundir la señal de datos con el ruido.

El proceso de conectarse a una red LAN inalámbrica, consiste de dos sub procesos separados. Estos sub procesos ocurren siempre en el mismo orden, y son llamados "autenticación y asociación".

4.1.10 Autenticación

El primer paso en el proceso de conexión a una LAN inalámbrica, es la autenticación. La autenticación es el proceso a través del cual un nodo inalámbrico (tarjeta de computadora, cliente USB, etc.) su identidad es verificada por la red. (Usualmente el punto de acceso) a la cual sé esta intentando conectar. Esta verificación ocurre cuando el punto de acceso al cual el cliente esta conectado verifica que el cliente es quien dice ser. Algunas veces el proceso de autenticación es nulo, significando esto que aunque ambos el cliente y el punto de acceso tienen que proceder a través de este paso para asociarse, no hay realmente una identidad especial requerida para el proceso de asociación

El cliente empieza el proceso de autenticación a través del envió de un frame de requerimiento de autenticación al punto de acceso (en el modo infraestructura). El punto de acceso puede aceptar o negar el requerimiento. Después de notificar a la estación su decisión con un frame de respuesta de autenticación, el proceso de autenticación puede ser realizado en el punto de acceso o el punto de acceso puede pasar esta responsabilidad a un servidor de autenticación tales como RADIUS. El servidor RADIUS entonces procesara la autenticación basada en los criterios de una lista, y entonces regresa el resultado al punto de acceso y así el punto de acceso puede regresar el resultado a la estación cliente.

4.1.11 Asociación

Una vez que le cliente ha sido autenticado, el cliente entonces es asociado tonel punto de acceso. Asociado, es el estado en el cual un cliente le es permitido pasar datos a través de un punto de acceso. Si una computadora con tarjeta de red inalámbrica esta asociada a un punto de acceso, entonces la tarjeta de red inalámbrica esta conectada al punto de acceso y por consiguiente a la red.

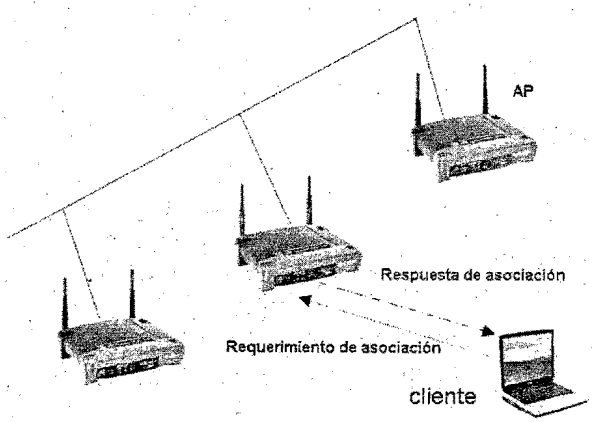


Figura 4.1.11-1 Asociación

El proceso de asociación es el siguiente. Cuando un cliente quiere conectarse, el cliente envía un requerimiento de autenticación al punto de acceso y recibe una respuesta de autenticación, después de que la autenticación ha sido completada, la estación envía un frame de requerimiento de asociación al punto de acceso que replica al cliente con un frame de respuesta de asociación permitiendo o negando la asociación.

El proceso completo de autenticación y asociación tiene tres distintos estados:

No-autenticación y no-asociación

Autenticación y no-asociación

Autenticación y asociación

4.1.12 No-autenticación y no asociación

En el estado inicial, el nodo inalámbrico esta completamente desconectado de la red y no puede pasar frames a través del punto de acceso. El punto de acceso mantiene una tabla del estatus de las conexiones de los clientes conocida como la tabla de asociación. Es importante hacer notar que los diferentes fabricantes se refieren al estado de no-autenticación y no-asociación en las tablas de asociación de sus puntos de acceso de forma diferente. Esta tabla típicamente mostrara "no-autenticación" para cualquier cliente que no ha completado el proceso de autenticación o ha intentado autenticarse y fallo.

4.1.13 Autenticación y no-asociación

En este segundo estado, los clientes inalámbricos han pasado el proceso de autenticación, pero todavía no están asociados con el punto de acceso. Al cliente todavía no le es permitido enviar o recibir datos a través del punto de acceso.

4.1.14 Autenticación y asociación

En este estado final, el cliente inalámbrico esta completamente conectado a la red y es capaz de enviar y recibir datos a través del punto de acceso a través del cual el nodo esta conectado (asociado).

Es importante hacer notar que un cliente inalámbrico móvil, puede autenticar a más de un punto de acceso a la vez, pero solo puede asociarse con un punto de acceso. Esta pre-autenticación hace más rápida y suave el Roaming cuando los clientes se mueven del área de cobertura de un punto de acceso a otra.

4.1.15 Métodos de autenticación

El estándar 802.11 especifica dos métodos de autenticación: autenticación de sistema abierto y autenticación con clave compartida. Esto es así tanto para dispositivos 802.11b como para dispositivos 8011.11a, 802.11g.

4.1.16 Autenticación de sistema abierto

La autenticación de sistema abierto es un método de autenticación nula y esta especificada en el estándar 802.11 como la configuración por default en los equipos WLAN. Usando este tipo de autenticación, una estación puede asociarse con cualquier punto de acceso que use autenticación de sistema abierto, basada solo en tener solo el SSID correcto. El SSID debe ser el mismo tanto en el punto de acceso como en el cliente.

4.1.17 Proceso de autenticación de sistema abierto

El proceso de autenticación de sistema abierto ocurre como sigue:

El cliente inalámbrico hace un requerimiento para asociarse al punto de acceso.

El punto de acceso autentica al cliente y envía una respuesta positiva, entonces el cliente es asociado a la red.

4.1.18 Autenticación de clave compartida

La autenticación de clave compartida es un método de autenticación que requiere del uso de WEP. La encriptación WEP usa clave que es ingresada en el cliente y en el punto de acceso, estas claves debe ser iguales a fin de que trabaje adecuadamente.

Proceso de autenticación de clave compartida.

El procese de autenticación usando autenticación de clave compartida ocurre como sigue:

Un cliente solicita asociación a un punto de acceso (este paso es el mismo, como el usado en autenticación de sistema abierto)

El punto de acceso emite un desafió al cliente, este desafió es aleatorio generando texto plano, el cual es enviado por el punto de acceso al cliente.

El cliente responde al desafió, el cliente responde encriptando el texto de desafió usando la clave WEP y envía esto al punto de acceso.

El punto de acceso responde a la respuesta del cliente, el punto de acceso des-encripta la respuesta encriptada del cliente para verificar que el texto de desafió fue encriptado con la clave WEP correcta. A través de este proceso el punto de acceso determina si en cliente tiene o no tiene la clave correcta. Si la clave WEP del cliente es la correcta el punto de acceso responderá positivamente y autenticara al cliente. Si la clave WEP del cliente no es la correcta el punto de acceso responderá negativamente y no autenticara al cliente, dejando al cliente sin autenticación y sin asociación al punto de acceso.

Hay muchas soluciones de autenticación seguras y protocolos en el Mercado de hoy, incluyendo VPN y 802.1x usando protocolo de autenticación extensible (EAP).

4.1.19 802.1x y EAP

El estándar 802.1x (control de acceso a la red basado en puertos) es relativamente nuevo y, los dispositivos que lo soportan tienen la habilidad de permitir una conexión hacia la red en la capa 2 solo si la autenticación es exitosa.

Típicamente, la autenticación de usuarios es realizada usando un servidor RADIUS y algún tipo de base de datos de usuarios (RADIUS nativo, active directory, etc.). En el modelo del estándar 802.11, la autenticación de red consiste de tres piezas: el solicitante, el autenticador y el servidor de autenticación.

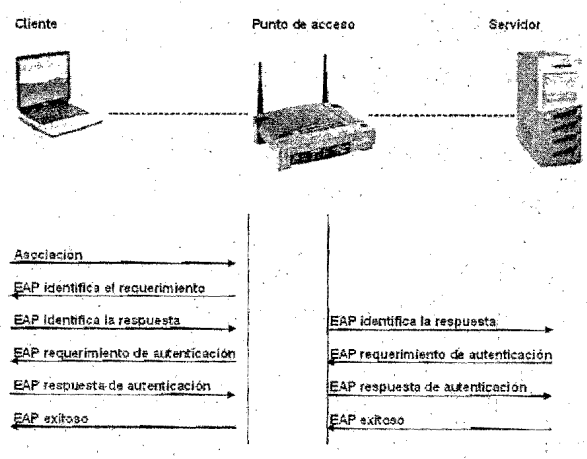


Figura 4.1.19-1 802.1x y EAP

4.2 Conjunto de servicios

El conjunto de servicios es un término usado para describir los componentes básicos para una red inalámbrica completamente operacional. En otras palabras, hay tres maneras de configurar redes WLAN en cada forma se requiere un conjunto de hardware. Las tres maneras de configurar una WLAN son:

Conjunto de servicios básicos (BSS)

Conjunto de servicios extendidos (ESS)

Conjunto de servicios básicos independientes (IBSS)

4.2.1 Conjunto de servicios básicos (BSS)

Cuando un punto de acceso es conectado a una red alambrada y un conjunto de estaciones inalámbricas, la configuración de la red es referida como un conjunto de servicios básicos (BSS). Un conjunto básico de servicios consiste solo de un punto de acceso y un o más clientes inalámbricos. Un BSS usa el modo infraestructura, un modo que requiere del usa de un punto de acceso en el cual todo el trafico inalámbrico pasa por el. No esta permitido conexiones directas de cliente a cliente. Cada cliente inalámbrico debe usar el punto de acceso para comunicarse con cualquiera del los otros clientes inalámbricos o host en la red por cable. El BSS cubre una célula simple, o área de RF, alrededor del punto de acceso con varias zonas de varias velocidades de transmisión.

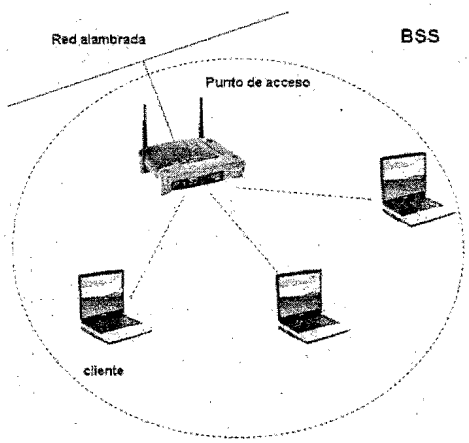


Figura 4.2.1-1 Conjunto de servicios básicos BSS

Las velocidades de estos círculos dependen de la tecnología empleada. A medida que nos alejemos del punto de acceso mas baja será la velocidad de transmisión de datos.

4.2.2 Conjunto de servicios extendidos (ESS)

Un conjunto de servicios extendidos (ESS) esta definido como dos o más conjuntos de servicios básicos (BSS) conectados a un sistema de distribución en común. El sistema de distribución puede ser por cable o inalámbrico, LAN, WAN, o cualquier otro método de conectividad de red. Una ESS debe tener al menos 2 puntos de acceso operando en el modo infraestructura. Similar a una BSS, todos los paquetes en una ESS deben de ir a través del punto de acceso.

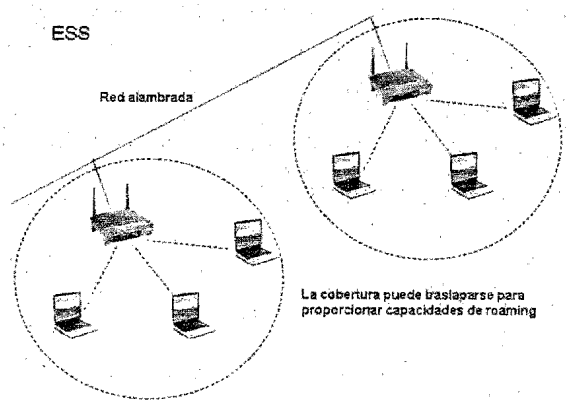


Figura 4.2.2-1 Conjunto de servicios extendidos ESS

Otra característica de una ESS, acorde con el estándar 802.11, es que una ESS cubre múltiples células, permitiendo, pero no requerido, capacidades de Roaming y no requiere usar un mismo SSID.

4.2.3 Conjunto de servicios básicos independientes (IBSS)

Un conjunto de servicios básicos independientes es también conocido como "red ad-hoc". Una IBSS no tiene un punto de acceso o cualquier otro tipo de acceso al sistema de distribución, pero cubre una célula simple y tiene un SSID. Los clientes en una IBSS alternan la responsabilidad de enviar las señales guía (beacon) debido a que no hay un punto de acceso para desarrollar esta tarea.

En orden de transmitir datos hacia fuera de una IBSS uno de los clientes en la IBSS debe actuar como Gateway o router, usando soluciones en software para este propósito. En una IBSS los clientes hacen conexiones directas a cada uno de los otros cuando transmiten datos.

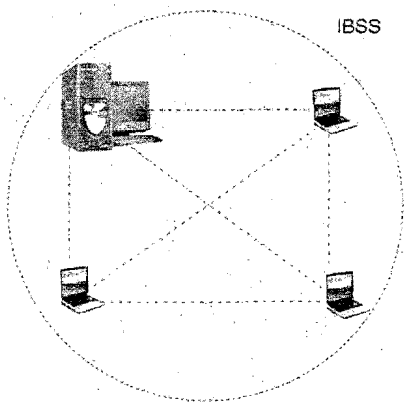


Figura 4.2.3-1 Conjunto de servicios básicos independientes IBSS

4.2.4 Roaming

Roaming es el proceso o habilidad de un cliente inalámbrico para moverse de una célula (o BSS) a otra sin perder la conectividad de la red. El punto de acceso maneja al cliente desde un uno a otro en una forma que es transparente para el cliente, asegurando que la conectividad no se rompa.

Cuando una área de una construcción esta dentro del área de cobertura de mas un punto de acceso, las coberturas de la células se traslapan. El traslape de las coberturas es un atributo importante de la configuración de las redes WLAN, debido a que permite el Roaming entre células traslapadas.

Cuando la cobertura de dos o más puntos de acceso se traslapa, las estaciones en el área traslapada pueden establecer la mejor conexión posible con uno de los puntos de acceso mientras continúan buscando por el mejor punto de acceso. Para reducir al mínimo la perdida de paquetes durante el switcheo, el anterior y el nuevo punto de acceso se comunican para coordinar el proceso de Roaming. Esta función es similar a la función handover en telefonía celular, con dos diferencias principales:

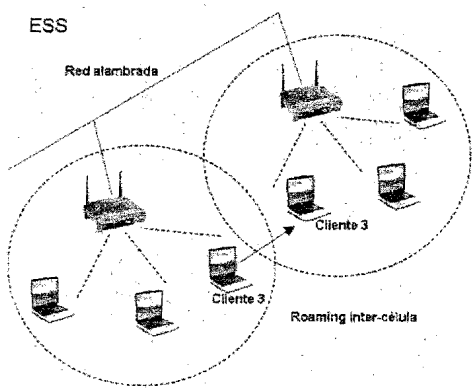


Figura 4.2.4-1 Roaming

En un sistema LAN basado en paquetes, la transición de una célula a otra célula puede ser desarrollada entre transmisión de paquetes, opuesto a la telefonía donde la transición puede ocurrir durante la conversación de voz.

En sistemas de voz, una desconexión temporal puede no afectar la conversación, mientras que en ambientes basados en paquetes, se reduce significativamente el rendimiento debido a que los protocolos de capas superiores retransmiten los datos.

El estándar 802.11 no define como el Roaming debe ser desarrollado, pero define los bloques básicos. Estos bloques básicos incluyen escaneo pasivo y activo y procesos de re-asociación. La re-asociación ocurre cuando una estación inalámbrica vaga de un punto de acceso a otro, volviéndose a asociar con el nuevo punto de acceso. Los clientes que se encuentran vagando usan las señales guía (beacon) para medir la fuerza de la señal de su conexión existente con el punto de acceso. Si la conexión es débil, la estación que vaga puede intentar asociarse el mismo con un nuevo punto de acceso.

El estándar intenta asegurar una disrupción mínima para la entrega de datos y proporciona algunas características para almacenar y enviar información entre BSS.

4.2.5 Re-asociación

La re-asociación usualmente ocurre debido a que una estación inalámbrica se ha movido físicamente en relación al punto de acceso original, causando esto que la señal se debilite. En otros casos la re-asociación ocurre cuando cambian las características de radio en las instalaciones, debido simplemente al alto tráfico de red en el punto de acceso original. En el ultimo caso, esta función es conocida como "balanceo de carga", debido a que su función principal es distribuir la carga total de la LAN inalámbrica lo mas eficientemente posible a través de la infraestructura inalámbrica disponible.

Asociación y re-asociación difieren solo ligeramente en su uso. Los frames de requerimiento de asociación son usados cuando se une un cliente a una red por primera vez. Los frames de requerimiento de re-asociación son usados cuando se vaga entre puntos de acceso así el nuevo punto de acceso se entera para la transferencia de negociación de frames intermedios desde el punto de acceso viejo y permite al sistema distribuido conocer que el cliente se ha movido.

4.2.6 Balance de carga

Áreas congestionadas con muchos usuarios y carga de tráfico pesado por unidad puede requerir una estructura multicelular. En una estructura multi-celular, algunos puntos de acceso en el mismo lugar, "iluminan" la misma área creando una cobertura común, la cual incrementa el manejo de trafico. Las estaciones dentro de la cobertura común, automáticamente se asocian con el punto de acceso que es menos cargado de tráfico y proporciona la mejor calidad de la señal. Balance de carga es conocido también como carga compartida y es configurada en ambos, las estaciones y los puntos de acceso.

4.3 Administración de potencia.

Los clientes inalámbricos operan en una de las dos modalidades de administración de potencia especificados por el estándar 802.11. Estos modos de administración de potencia son: modo activo, el cual es comúnmente llamado "modo consiente continuo" (CAM).y modo de ahorro, que es comúnmente llamado "modo de sondeo de ahorro de energía (PSP). Este último modo es muy importante para los usuarios móviles que usan dispositivos con baterías. Extiende la vida de las baterías permitiendo a los usuarios trabajar sin necesidad de recargar constantemente la batería.

4.3.1 Modo conciente continuo (CAM)

El modo conciente continuo es la configuración durante la cual los clientes inalámbricos usan la potencia completa, no pasa la tarjeta a modo de "dormir" y esta en constante comunicación con el punto de acceso.

4.3.2 Modo de sondeo de ahorro de energía (PSP)

Usando modo de sondeo de ahorro de energía permite a los clientes inalámbricos entrar en el modo "dormir". Dormir significa que el cliente actualmente pasa su

estado de baja potencia por algún periodo de tiempo, quizás algunas fracciones de segundo. Este periodo de dormir es suficiente para ahorrar una cantidad significante de energía en el cliente inalámbrico.

Cuando se usa PSP, los clientes inalámbricos se comportan de forma distinta entre el conjunto de servicios básicos (BSS) y el conjunto de servicios básicos independientes. La única similitud en las habilidades de una BSS y un IBSS es el envió y recepción de señales guía (beacon).

4.3.3 PSP en el conjunto de servicios básicos

Cuando se usa PSP en una BSS, la estación primero envía un frame al punto de acceso para informar al punto de acceso que va a pasar a l modo de "dormir". El punto de acceso entonces recuerda a la estación como "dormida". El punto de acceso guarda cualquier frame que sea destinad para la estación "dormida". El trafico para estos clientes quienes están "durmiendo" continúan llegando al punto de acceso, pero el punto de acceso no puede enviar trafico a clientes durmiendo. Por lo tanto, los paquetes quedan encolados en un buffer marcado para el cliente durmiendo.

El punto de acceso esta constantemente enviando señales guía (beacon) en un intervalo regular. Desde que un cliente esta sincronizado con el punto de acceso, sabe exactamente cuando recibir las señales guía (beacon). Los clientes que están durmiendo, encenderán sus receptores para escuchar las señales guía (beacon), que contiene el mapa de indicación de trafico (TIM). Si una estación ve que esta listada en el TIM, su receptor se enciende y envía frame al punto de acceso notificándole que el ahora esta "despierto" y listo para recibir los paquetes de datos almacenados. Una vez que el cliente ha recibido sus paquetes desde el punto de acceso, el cliente envía un mensaje al punto de acceso informándole que el cliente esta regresando al modo de "dormir". Este proceso se repite una y otra vez. Este proceso crea algo de sobre carga que puede no estar presente si el modo PSP no fuera inicializado.

4.3.4 PSP en un conjunto de servicios básicos independientes

El proceso de comunicación con ahorro de energía en una IBSS es muy diferente en relación al usando en una BSS. En una IBSS no hay punto de acceso, así no hay dispositivo para almacenar los paquetes. Por lo tanto cada estación debe almacenar paquetes destinados desde el mismo a cualquier otra estación en una red Ad-hoc. Las estaciones alternan el envió de señales guía (beacon) en una IBSS usando varios métodos, cada uno dependiendo de el fabricante de equipo.

Cuando una estación esta usando el modo de ahorro de energía, hay un periodo de tiempo llamado ventana ATIM, durante el cual cada estación esta completamente despierta y lista para recibir frame s de datos. El mensaje de indicación de trafico Ad-hoc (ATIM) es un frame unicast usado por las estaciones para notificar a las otras estaciones que hay datos destinados a ellos y que ellas deberían mantenerse despiertas lo suficiente para recibir los datos.

Los ATIM y las señales guía (beacon) son enviados durante la ventana ATIM. El proceso seguido por las estaciones para pasar trafico para pasar tráfico entre cliente es:

Las estaciones son mantenidas por el estándar para estar despiertas durante todas las señales guía (beacon). Ellas no pueden dormir por más de un periodo de señales guía (beacon). Debido a este hecho, todas las estaciones estarán "despiertas" antes de que el periodo que la ventana ATIM empiece.

Empieza la ventana de ATIM, una estación designada envía una señal guía (beacon) y entonces envía a las estaciones los frames de ATIM notificando a otras estaciones del tráfico almacenado destinado para ellas.

Las estaciones reciben los frames de ATIM durante la ventana de ATIM manteniéndose encendidos los receptores durante este tiempo para recibir los frames de datos. Si no son recibidos los frames de ATIM, las estaciones pueden

regresar al estado de "dormido" hasta la siguiente señal guía (beacon) inicie y la ventana de ATIM vuelva a iniciar otra vez.

La ventana ATIM se cierra, y la estación empieza transmitiendo sus frames de datos a las otras estaciones, después de haber recibido los frames de datos, reinician el ciclo hasta el siguiente ventaneo de ATIM.

4.4 Comunicación en las WLAN

Una vez que un cliente se ha unido a la red, el cliente y el resto de la red se comunicara pasando a través de la red, en la mayoría en la misma manera como cualquier otra red IEEE 802, pero las WLAN no usan los frames Ethernet 802.3.

Hay tres distintos tipos de frames inalámbricos en las WLAN: control, administración y datos. Cada uno de los frames es construido de forma distinta y transportan información relacionada a su nombre. Los frames de las WLAN tienen un tamaño máximo de 2346 bytes (de los cuales 2312 son disponibles para transportar datos antes de que el estándar 802.11 requiera fragmentar. Sin embargo los frames inalámbricos son generalmente fragmentados a 1518 bytes por el punto de acceso debido a la travesía de los datos en los entre los medios alambrados (Ethernet 802.3) e inalámbricos (802.11). Los frames de alambrados (Ethernet) tiene un tamaño máximo de 1518 bytes (de los cuales 1500 bytes son disponibles para trasportar datos), debido a esta razón los frames inalámbricos son típicamente fragmentados a 1518 bytes.

El preamble (una serie de bits ceros o unos utilizados para sincronización en el inicio de cada frame, es siempre enviado a 1 Mbps para proporcionar una velocidad de transmisión común que cualquier receptor pueda interpretar. Hay dos tamaños de preamble (también llamados PLCP preamble) largo de 128 bits y corto de 56 bits. Es importante que cada terminación de nodo de un enlace inalámbrico use el mismo tipo de preamble. Después de que el preamble es enviado, el encabezado (header también llamado PLCP, protocolo de convergencia de capa física) es enviado. Para preamble largos, el preamble y el header son ambos enviados a 1 mbps, para

preamble cortos, el preamble es enviado a 1 Mbps y el header es enviado a 2 Mbps. El campo de velocidad de datos en el encabezado especifica la velocidad a la cuál los datos serán transmitidos. Después de enviar el encabezado, el transmisor puede entonces cambiar la velocidad de datos al valor que especifica el encabezado. Lo mismo aplica a las señales guía (beacon) que son enviados a 1 Mbps por las mismas razones.

Hay tres diferentes categorías de frames generados dentro de todos los formatos. Estas tres categorías y sus tipos dentro de cada categoría son:

Frames de administración

Frame de requerimiento de asociación

Frame de respuesta de asociación

Frame de requerimiento de re-asociación

Frame de respuesta de re-asociación

Frame de requerimiento de prueba

Frame de respuesta de prueba

Frame de beacon (señales guía)

Frame de ATIM

Frame de dis-asociación

Frame de autenticación

Frame de des-autenticación

Frames de control

Requerimiento para enviar (RTS)

Libre para enviar (CTS)

Reconocimientos (ACK)

Poleo de ahorro de potencia (PSP)

contención-terminación libre (CF terminación)

CF end + CF ack

Frames de datos

Datos

Cierto tipo de frames usan ciertos campos dentro de todo el frame. Lo que todo administrador de redes inalámbricas debe saber es que las redes WLAN soportan prácticamente todos protocolos de las capas 3 a 7 como: IP, IPX, NetBEUI, Apple Talk, RIP, DNS, FTP, etc. la principal diferencia contra el Ethernet 802.3 esta implementada en la capa de control de acceso al medio (MAC) sub-capa de la capa de enlace de datos y en toda la capa física. Los protocolos superiores simplemente son considerados carga útil por la capa 2 de los frames inalámbricos.

4.4.1 Manejo de colisiones

Desde que la radio frecuencia es un medio compartido, las redes WLAN tienen que tratar con la posibilidad de colisiones de la misma manera que una red alambrada tradicional lo hace. Esto no significa que una estación que envía pueda determinar que esta a teniendo una colisión. Es imposible detectar una colisión en la WLAN. Por esta razón las WLAN utilizan el protocolo de evasión de colisión/ acceso múltiple por detección de portadora (CSMA/CA).

La gran diferencia entre CSMA/CA y CSMA/CD es que CSMA/CA evita las colisiones y usa reconocimientos positivos (ACK). Cuando una estación inalámbrica envía un paquete, la estación que recibe envía un reconocimiento (ACK) hacia el origen del paquete una vez que el paquete ha sido recibido. Si la estación que envió el paquete no recibe el reconocimiento (ACK), la estación que envió entonces asume que hubo una colisión y re-envía los datos.

CSMA/CA adiciona una gran cantidad de datos de control usados por las WLAN, causan un excesivo uso de encabezados en los frames, aproximadamente el 50 % del ancho de banda de una WLAN.

El protocolo CSMA/CA evita la probabilidad de colisión entre estaciones compartiendo el medio a través del uso de un tiempo aleatorio de retorno si las estaciones físicas o lógicas envían mecanismos indicando un medio ocupado. El periodo de tiempo inmediatamente seguido a un medio ocupado es cuando la alta probabilidad de colisión ocurre, especialmente durante la lata utilización. En este punto de tiempo, muchas estaciones pueden estar esperando por el uso del medio e intentara transmitir en el mismo tiempo. Una vez que el medio es libre, el tiempo aleatorio de retorno difiere entre las estaciones minimizando las probabilidades de colisión.

4.4.2 Fragmentación

La fragmentación de paquetes en pequeños fragmentos adiciona encabezados excesivos y reduce la eficiencia de protocolo cuando no son observados errores, pero reduce el tiempo invertido en la retransmisión si ocurren errores. Paquetes largos tienen una alta probabilidad de colisión en la red, por lo tanto un método para variar el tamaño de los paquetes es necesario. El estándar 802.11 proporciona soporte para fragmentación. A través de disminuir la longitud de cada paquete, la probabilidad de interferencia durante la transmisión de paquetes, puede reducirse. Este en un acuerdo que debe hacerse entre la baja razón de errores de paquetes que pueden ser alcanzadas usando paquetes cortos y el uso excesivo de

encabezados de mas frames en la red debido a la fragmentación. Cada fragmento requiere su propio encabezado y reconocimiento (ACK), así el ajuste del nivel de fragmentación, es también un ajuste en la cantidad de encabezados asociados con cada paquete transmitido. Las estaciones nunca fragmentan frames de multi-cast y broadcast, pero si, solo frames de unicast para no introducir sobre encabezados excesivos en la red. Buscar la configuración de fragmentación optima para maximizar la entrega de datos en la red, es un punto muy importante para la administración de redes WLAN. Mantengamos en mente que los frames de 2346 bytes es el mas largo que puede atravesar segmento de LAN inalámbrica sin fragmentación. Aunque muchos puntos de acceso fragmentaran cualquier frame mayor a 1518 bytes antes de ponerlos en el segmento alambrado.

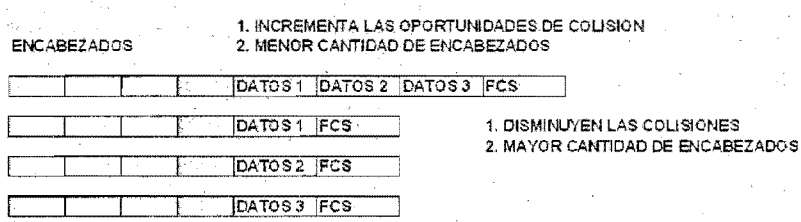


Figura 4.4.2-1 Fragmentación

Una manera de usar la fragmentación para mejorar la entrega de datos en la red en momentos de altos errores de paquetes es monitorear la razón de errores de paquetes en la red y ajusta el nivel de fragmentación manualmente, esto en el cliente y/o en el punto de acceso (dependiendo de cual dispositivo permita hacer esto).

4.4.3 Fragmentación de ráfaga

El estándar 802.11 permite a los frames ser fragmentados en pequeñas piezas. Cada fragmento es numerado de manera única y son reconocidos por el recipiente. En esta manera la estación que esta enviando, no puede transmitir el siguiente fragmento hasta que el previo fragmento haya sido reconocido por el receptor. Sin

embargo una vez que el canal ha sido adquirido vía los mecanismos de RTS y CTS, pueden ser enviados múltiples fragmentos en una fila.

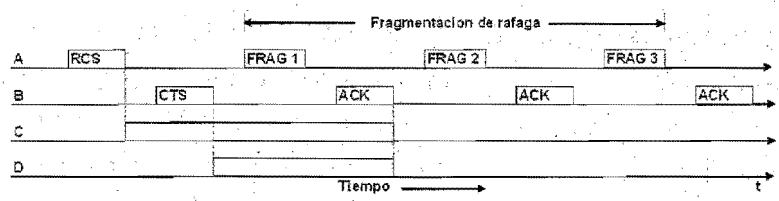


Figura 4.4.3-1 Fragmentación de ráfaga

Típicamente los mecanismos NAV (vector de asignación de red) solo mantienen de transmitir a las otras estaciones hasta que el siguiente ACK es recibido. La fragmentación de ráfaga permite a un fragmento de ráfaga completo ser enviado sin ser interferido o interrumpido.

4.4.4 Fragmentación dinámica de razón de cambio (DRS)

La selección de velocidad adaptativa (ARS) y cambio de velocidad dinámico (DRS) son términos usados para describir el método de ajuste de velocidad dinámica en cliente de una red WLAN.

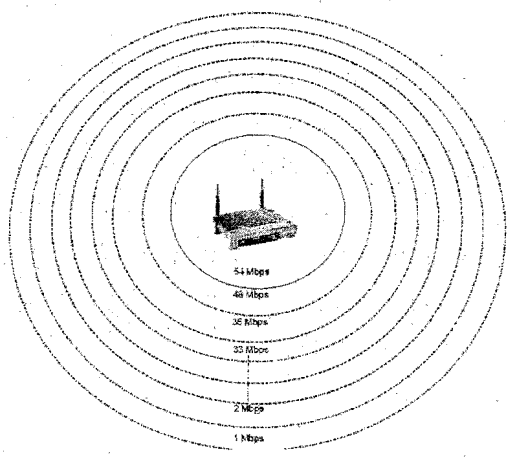


Figura 4.4.4-1 Cambio de velocidad dinámico

Este ajuste de velocidad ocurre como una función del incremento de la distancia entre el cliente WLAN y el punto de acceso o con el incremento de la interferencia, y solo hace saltos entre las velocidades de transmisión establecidas en el estándar 802.11, por ejemplo si una estación con una velocidad de transmisión de datos de 11 mbps incrementa su distancia paulatinamente, su velocidad empezara a decrecer primero a 5.5 Mbps, después a 2 Mbps y por ultimo a 1 mbps hasta perder comunicación con el punto de acceso.

4.4.5 Función de coordinación distribuida (DCF)

La función de coordinación distribuida (DCF) es un método de acceso especificado en el estándar 802.11 que permite a todas las estaciones en una red inalámbrica, luchar por acceso en un medio de transmisión compartido (RF) usando el protocolo CSMA/CA. En este caso el medio de transmisión es una porción de la banda de

radio frecuencia. Los BSS, ESS y los IBSS pueden todos usar el modo DCF. El punto de acceso en estos conjuntos de servicios actúa en la misma forma como el estándar 802.3 basado en hub alambrados para transmitir datos, y DCF es el modo en el cual el punto de acceso envía los datos.

4.4.6 Función de coordinación de punto

La función de coordinación de punto (PCF) es un modo de transmisión permitido para la libre contención de frames en una LAN inalámbrica a través de hacer uso de mecanismos de poleo. PCF tiene la ventaja de garantizar una cantidad conocida de latencia de aplicaciones que así requieren QoS (voz, video por ejemplo) para poder ser usados. Cuando es usado el PCF, el punto de acceso en una red inalámbrica desarrolla el poleo. En una red ad-hoc no se puede hacer uso del PCF por que este se implementa solo en el punto de acceso.

4.4.7 El proceso de PCF

Primero, una estación inalámbrica debe decir al punto de acceso que la estación es capaz de responder el poleo, entonces el punto de acceso pregunta, o polea, cada estación inalámbrica para ver si las estaciones necesitan enviar frames de datos a través de la red. PCF, a través del poleo, genera una cantidad significativa encabezados en una red WLAN.

DCF puede ser usada sin PCF, pero PCF no puede ser usada sin DCF. DCF es escalable debido a su diseño basado en contención, mientras que PCF, por diseño, limita la escalabilidad de una red inalámbrica porque adiciona una cantidad de encabezados adicionales de frames de poleo.

4.4.8 Espaciamiento inter-frame

El espaciamiento inter-frames es el termino usado para referirse a un espacio de tiempo estandarizado que es usado en todas las redes WALN 802.11.

Hay tres tipos principales de intervalos de espaciamientos (espacios inter-frame) SIFS, DIFS y PIFS. Cada tipo de espacio inter-frames es usado por cualquier redes WLAN para enviar cierto tipo de mensajes a través de al red o para administrar el intervalo durante el cual la estación contiende por el medio de transmisión.

El espacio inter-frame es medio en micro segundos y es usado para diferir un acceso de una estación a el medio y para proporcionar varios niveles de prioridad. En una red inalámbrica, cualquier cosa es sincronizada y todas las estaciones y puntos de acceso usan cantidades de tiempo estándar (espacios) para desarrollar varias tareas. Cada nodo conoce estos espacios y los usa apropiadamente, par realizar ciertas acciones en la red.

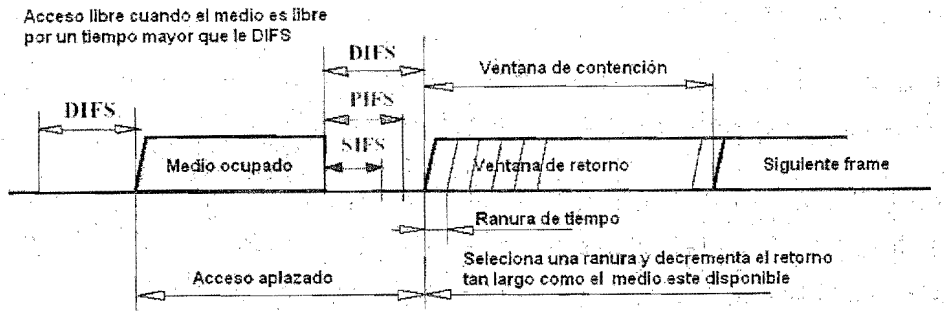


Figura 4.4.8-1 Espacios inter-frame

4.4.9 Espacios inter-frame cortos (SIFS)

SIFS es un espacio de tiempo antes y después del cual el siguiente tipo de mensaje es enviado. SIFS proporciona el alto nivel de prioridad en una red inalámbrica. La razón para que SIFS tenga la alta prioridad es que las estaciones constantemente escuchan el medio (detección de portadora) esperando un medio limpio (no ocupado). Una vez que el medio es libre, cada estación debe esperar una cantidad de tiempo dado (espacio) antes de proceder con una transmisión. La duración del tiempo que una estación deba esperar esta determinado por la función que la estación necesite realizar. Cada función en una red inalámbrica cae en las categorías de espaciamiento.

4.4.10 Punto de coordinación de la función de espacio inter-frame (PIFS)

El PIFS toma más prioridad que el DIFS y menos que SIFS. Los puntos de acceso usan un espacio inter-frame PIFS solo cuando la red esta en el modo de función de coordinación de punto, es cual es manualmente configurado por el administrador. PIFS es mas corto en duración que DIFS, así el punto de acceso siempre ganara el control de el medio antes de que otra estación contendiente en un modo de función de coordinación distribuida (DCF). PCF solo trabaja con DCF no como un modo de operación solo (stand-alone) así que, cuando el punto de acceso a finalizado su

poleo, las otras estaciones pueden continuar por la contención por el medio de transmisión usando el modo DCF.

4.4.11 Coordinación distribuida de la función de espacios inter-frame (DIFS)

DIFS es el mas largo de los espacios de frames y es usado por default en todas las estaciones que cumplen con el estándar 802.11 que están usando la función de coordinación distribuida. Cada estación en la red usando el modo DCF es requerido para esperar hasta que el DIFS ha expirado antes de que cualquier estación pueda contender por la red. Todas las estaciones operando acorde con DCF, usan DIFS para transmitir frames de datos y frames de administración. Estos espacios hacen la transmisión de estos frames de baja prioridad en relaciona las transmisiones basadas en PCF. En lugar de que todas las estaciones asuman que el medio es libre y arbitrariamente empiecen transmitiendo simultáneamente después de DIFS (el cual causaría colisión), cada estación usa un algoritmo de tiempo aleatorio para determinar cuanto tiempo esperar antes de enviar sus datos.

El periodo de tiempo seguido a DIFS es referido como el periodo de contención (CP). Todas las estaciones en el modo DCF usan un algoritmo aleatorio de retorno durante el periodo de contención. Durante el periodo de retorno aleatorio, una estación elije un numero aleatorio y lo multiplica por la ranura de tiempo para conseguir la longitud de tiempo que esperara. Las estaciones cuentan hacia abajo esta cantidad de tiempo de retorno aleatorio uno por uno, desarrollando un CCA (valoración de canal libre) después de cada ranura de tiempo para ver si el medio esta ocupado. Cualquiera de las estaciones a la cual su contador regrese a cero primero, realizara un CCA, para que se le asigne un medio libre y su vector de asignación de red (NAV) esta en cero, para empezara a trasmitir.

Una vez que la primer estación empezó a transmitir, todas las otras estaciones censaran que el medio este ocupado, y recuerdan su tiempo de regreso aleatorio restante del previo CP. La restante cantidad de tiempo es usada en lugar de levantar

otro número aleatorio durante el siguiente CP. Este proceso asegura el justo acceso al medio a todas las estaciones.

Una vez que el periodo de tiempo de retorno ha terminado, la estación transmisora envía sus datos y recibe de regreso un ACK (reconocimiento) desde la estación receptora. Este proceso entero se repite.

4.4.12 Ranuras de tiempo

Una ranura de tiempo la cual es pre-programada en el radio en el mismo modo como lo es las estructuras de tiempo SIFS, PIFS y DIFS, es un periodo de tiempo estándar en la red inalámbrica. La ranura de tiempo es usada dentro del CP en la misma forma que la segunda aguja de un reloj es usada. Un nodo inalámbrico marca las ranuras de tiempo similar a como un reloj marca los segundos. Estas ranuras de tiempo son determinadas por la tecnología de red inalámbrica usada.

1. ranura de tiempo para FHSS = 50 us
2. ranura de tiempo para DSSS = 20 us
3. ranura de tiempo para infrarrojo = 8 us

Además:

1. PIFS = SIFS + 1 ranura de tiempo
2. DIFS = PIFS + 1 ranura de tiempo

También si revisamos el periodo de tiempo de la ranura de tiempo en FHSS es muy larga, también el tiempo DIFS y el tiempo PIFS en relación a DSSS. Estos periodos de tiempo largos contribuyen al sobre encabezado de la trama lo cual disminuye la entrega de datos.

4.4.13 El proceso de comunicación

Los puntos de acceso no tienen que esperar por un DIFS, pero las estaciones si. Esto es cierto, excepto por la existencia de algo llamado súper-frame. Un súper frame es un periodo de tiempo y este consiste de dos partes:

1. periodo de libre contención (CFP), el cual incluye a los beacons.
2. periodo de contención (CP).

Un diagrama del súper-frame se muestra en la Figura 4.4.13-1, el propósito del súper-frame es permitir la pacifica y justa co-existencia entre los modos PCF y DCF en los clientes de la red, permitiendo calidad de servicio (QoS) a algunos pero no a otros.

Otra vez recordando que PIFS y por lo tanto los súper-frames solo ocurren cuando:

1. la red esta en el modo de función de punto de coordinación
2. el punto de acceso ha sido configurado para hacer poleo (sondeo).
3. los clientes inalámbricos han sido configurados para anunciar al punto de acceso que ellos están poleando (sondeando).

Por lo tanto si empezamos desde un punto de inicio hipotético en una red que tiene el punto de acceso configurado para modo PCF, y entonces algunos de los clientes están configurados para poleo, el proceso es el siguiente:

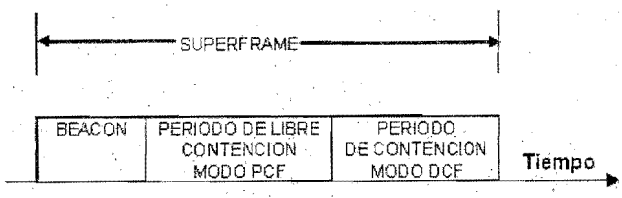


Figura 4.4.13-1 Súper-frame

1. El CFP empieza y el punto de acceso hace un broadcast con un beacon.
2. Durante el periodo de libre contención, el punto de acceso sondea a las estaciones para ver si alguna estación necesita enviar datos.
3. Si una estación necesita enviar datos, esta envía un frame hacia el punto de acceso en respuesta al sondeo del punto de acceso.
4. Si una estación no necesita enviar datos, esta regresa un frame nulo al punto de acceso en respuesta al sondeo del punto de acceso.
5. El sondeo (poleo) continúa a través del periodo de libre contención.
6. Una vez que el periodo de libre contención (CFP) termina y el periodo de contención (CP) empieza (denotado por el envió de una terminación de frame CF por el punto de acceso), el punto de acceso deja de polear a las estación. Durante el periodo de contención (CP), las estaciones y el punto de acceso usa el modo DCF para contender por el medio.
7. La súper-frame termina con la terminación del CP y un nuevo súper-frame empieza con el siguiente CFP.

El CFP es usado como un "política de acceso controlado" y el CP es usado como una "política de acceso aleatorio". Durante el CFP, el punto de acceso esta en completo control de todas las funciones de la red inalámbrica, mientras que durante el CP, cualquier estación arbitraria y aleatoriamente ganan el control sobre el medio. El punto de acceso en el modo de PCF (función de coordinación de punto) , no tiene que esperar por un DIFS que expire, pero usa el PIFS, el cual es mas corto que el DIFS para capturar el medio antes que cualquier cliente usando el modo DCF lo haga. Después de que el punto de acceso captura el medio y empieza poleando

transmisiones durante el CFP, el cliente DCF detecta el medio como ocupado y espera para transmitir. Después del CFP, el CP empieza, durante el cual todas las estaciones usando el modo DCF pueden contender por el medio y el punto de acceso conmuta al modo DCF. Cada beacon enviado por un punto de acceso durante el CFP, tiene el NAV puesto con suficiente cantidad e tiempo para completar el CFP. Este es el principal mecanismo para mantener a los clientes en el modo DCF callados durante el CFP.

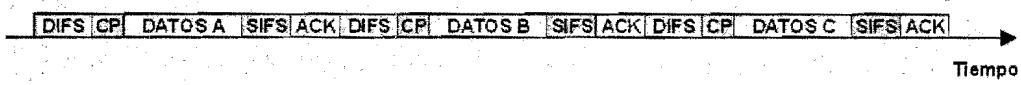


Figura 4.4.13-2 Línea de tiempo DCF

El proceso es algo más simple cuando una red inalámbrica esta en el modo DCF, debido a que no hay poleo y por lo tanto no hay súper-frame, este proceso es el siguiente:

1. las estaciones esperan por un DIFS que expire.
2. durante el CP el cual inmediatamente sigue a un DIFS, las estaciones calculan su tiempo de retorno aleatorio basados en un numero aleatorio multiplicado por una ranura de tiempo.
3. las estaciones cuanta hacia abajo su tiempo aleatorio con cada paso de ranuras de tiempo, chocando el medio (CCA) en la terminación de cada ranura de tiempo. La estación con el tiempo mas corto gana el control del medio primero que cualquier otra estación.
4. la estación envía sus datos.
5. la estación receptora recibe los datos y espera un SIFS antes de regresar un ACK hacia la estación que esta transmitiendo los datos.
6. la estación transmisora recibe el ACK y el proceso empieza desde el inicio con un nuevo DIFS.

4.4.14 Requerimiento para enviar /libre para enviar (RTS/CTS)

Hay dos mecanismos de detectan la portadora usados en redes inalámbricas. El primero es la detección de portadora física. La detección de portadora física funciona a través de revisar la fuerza de la señal. Llamado el indicador de fuerza de la señal recibida (RSSI), en la señal portadora de RF para ver si hay una estación actualmente transmitiendo. La segunda es la detección de portadora virtual. La detección de portadora virtual trabaja a través del uso de un campo llamado el vector de asignación de red (NAV), el cual actúa como un contador de la estación. Si una estación quiere transmitir su intención para usar la red, la estación envía un frame a la estación destino, la cual establecerá el campo NAV en todas las estaciones escuchando el frame con el tiempo necesario para que la estación complete su transmisión más el retorno del frame de ACK. De esta manera cualquier estación puede reservarse el uso de la red por un periodo de tiempo. La detección de portadora virtual es implementada con el protocolo RTS/CTS.

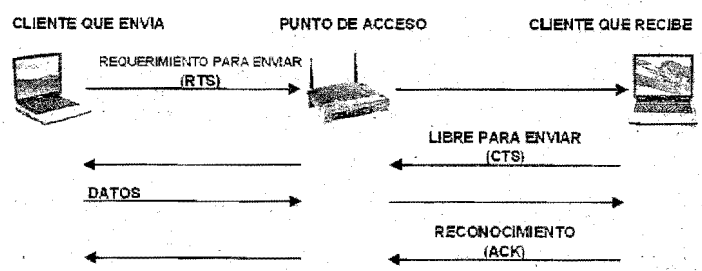


Figura 4.4.14-1Protocolo RTS/CTS

El protocolo RTS/CTS es una extensión del protocolo CSMA/CA, es te protocolo es utilizado para resolver problemas como de "nodo oculto". Usando RTS/CTS se le permite a las estaciones transmitir su intento de envió de datos a través de la red.

RTS/CTS causara significativo sobre encabezados en la trama inalámbrica de WLAN. Por esta razón RTS/CTS esta configuradò en modo apagado por default en las LAN inalámbricas. Si se esta experimentando una inusual cantidad de colisiones

en una Lan inalámbrica (evidenciado por los altos retardos y la baja transferencia de información), usando RTS/CTS puede incrementarse el flujo de tráfico en la red debido a que disminuye el número de colisiones.

La Figura 4.4.14-1 ilustra los cuatro pasos del proceso de dialogo para CTS/RTS. La estación transmisora envía su RTS seguido de CTS replicado por la estación receptora, los cuales pasan a través del punto de acceso (ambos RTS y CTS). Después la estación transmisora envía sus datos a través del punto de acceso a la estación receptora que inmediatamente replica con un frame de reconocimiento (ACK). Este proceso es usado por cada frame que es enviado a través de la red inalámbrica.

Hay tres modalidades de configuración para la mayoría de los puntos de acceso y sus nodos para el uso de RTS/CTS:

1. apagado
2. encendido
3. encendido con umbral

Cuando RTS/CTS esta encendido cada paquete que va a través de la red inalámbrica es anunciado liberado entre el nodo transmisor y el nodo receptor antes de ser transmitido, creando un cantidad significativa de sobre encabezados y disminuyendo la entrega de datos. Generalmente RTS/CTS debe ser solo usado en problemas diagnosticados de la red y cuando paquetes muy largos están fluyendo a través de una red inalámbrica congestionada.

La configuración de encendido con umbral permite controlar que paquetes (sobre un cierto tamaño) son anunciados y liberados para enviarse por una estación. Debido a que las colisiones afectan más a los paquetes grandes que a los chicos, se puede configurar el umbral de RTS/CTS para trabajar solo cuando un nodo quiere enviar un paquete de un tamaño considerable, esto optimiza la entrega de datos en la red inalámbrica mientras que previene los problemas como el nodo oculto.

4.5 Protocolos de redes inalámbricas

Sobre los recientes años el Mercado de comunicaciones inalámbricas ha crecido enormemente. Las tecnologías inalámbricas ahora pueden ser encontradas virtualmente en cualquier lugar de la faz de la tierra. Cientos de millones de personas intercambian información cada día usando pager, teléfonos celulares y otros tipos de dispositivos de comunicación inalámbrica. Con tremendo éxito de la telefonía celular y los servicios de mensajes, es fuertemente sorprendente que las comunicaciones inalámbricas esta siendo aplicados al reino de la computación personal y de negocios. Las personas serán capaces de accesar y compartir información a una escala global por poco en cualquier lugar.

Desde el éxito del el proyecto Ethernet por el centro de investigación de Palo Alto de Xerox, en los inicios de los años 70´s, y otros similares protocolos, la tecnología básica esta siendo puesta para las redes de área local (LAN) para florecer en ambos sectores, el publico y el privado. Protocolos de redes LAN estándar, como el Ethernet, que opera con bastante alta velocidad con conexiones de hardware no costosas pueden traer redes digitales a la mayoría de las computadoras. Hoy en día, organizaciones de cualquier tamaño, accedan y comparten información sobre redes digitales. El poder de interconectar, colaborar, y distribuir computo esta empezando a ser realidad. Sin embargo hasta recientemente, las LAN eran limitadas físicamente por las infraestructuras de cableados de los edificios. Cualquiera con nodos de red de teléfonos de dial up, estaba limitado a acceder a través de una conexión por alambre, conexiones de líneas tendidas en tierra. Muchos usuarios de red, especialmente usuarios móviles en negocios, profesionistas médicos, fábricas y universidades por nombrar algunos, encuentran beneficios desde la adición de las capacidades inalámbricas de las LAN.

La mayor motivación y beneficio de las redes LAN inalámbricas es el incremento en la movilidad. No sujeto a las conexiones de red convencionales, los usuarios de red pueden moverse sobre la mayoría de los sitios sin restricciones y disponer de acceso a la red poco a poco desde cualquier sitio. Ejemplos de usos prácticos de las

redes de acceso inalámbricas, son solo limitadas por la imaginación del diseñador de la aplicación. Profesionales médicos pueden obtener no solo el historial de sus pacientes, sino también signos vitales de tiempo real y otros datos de referencia en la cabecera del paciente sin depender de documentos en papel como una libreta de notas. En las fábricas los trabajadores pueden acceder partes y especificaciones del proceso sin conexiones de red por cable impracticas y en algunos casos hasta imposibles. Conexiones inalámbricas con monitoreo de tiempo real, permiten a ingenieros remotos diagnosticar y dar mantenimiento para mantener el bienestar del equipo de manufactura, incluso en un ambiente hostil de una fabrica de manufactura de equipo los inventarios de almacén pueden ser transportados y verificar rápidamente y efectivamente con escáneres inalámbricos conectados a la base de inventario principal.

En adición a la incrementada portabilidad, LAN inalámbricas ofrecen incrementada flexibilidad. En algunos casos son más económico el uso de redes LAN inalámbricas. Para sitios como edificios viejos, fábricas donde no es factible correr un tendido de alambre para hacer una LAN tradicional, es más conveniente instalar una red inalámbrica, ofreciendo la conectividad y conveniencia de las redes por cable sin la necesidad de costosas instalación de cable.

4.5.1 Protocolos de redes inalámbricas

Debido al crecimiento de las redes inalámbricas hay un amplio rango de excelentes productos y protocolos disponibles para oficina u hogar. Ejemplos de esta diversidad son la primera generación de telefonía celular que pueden comunicarse a aproximadamente 9600 bps y hasta 54 Mbps ofrecidos por el estándar 802.11a.

Para complicar más esto cada una de estas tecnologías tiene su propio mercado y su correspondiente dispositivo propietario, además de forzar a usar su propio hardware y software. Que puede ser incompatible con otro dispositivo inalámbrico.

4.5.2 Fundamentos de redes

Mucho tiempo antes de que las redes inalámbricas fueran de uso como en ambientes Ethernet, el instituto de ingenieros eléctricos y electrónicos (IEEE) ha establecido un sistema por el cual nuevas tecnologías pueden ser certificadas. Las certificaciones de la IEEE aseguran que una nueva tecnología puede ser compatible con otros productos usando la misma tecnología certificada.

Una de las muchas tecnologías que fue y paso a través de estos procesos de revisión y certificación fueron la redes de área local (LAN). LAN es un grupo simple local de computadoras y su correspondiente hardware y software para facilitar la comunicación entre estas computadoras. Sin embargo hay un número de reglas y especificaciones que son requeridas para que un producto pueda ser juzgado como que cumple con LAN.

Así para manejar este especifico sector de tecnología, el IEEE creo el grupo 802, el cual es responsable de las revisiones de las tecnologías de redes viejas y nuevas para asegurar que son confiables y libres de conflictos. Si una nueva tecnología es lanzada para su certificación, es intensamente analizada por este grupo, y es puesta a muchas pruebas antes de que sea juzgada como respetable.

Las certificaciones 802 incluyen muchas subdivisiones, que representan diferentes facetas de las redes. Por ejemplo 802.3 es el estándar que define como trabaja Ethernet. Esto nos lleva a Ethernet inalámbrico, que es clasificado dentro del estándar 802.11.

En adición a esto 802.11 es dividido en varias especificaciones de certificaciones, como: 802.11a, 802.11b, 802.11g y otras que están por venir. Cada una de estas define diferentes métodos de proporcionar Ethernet inalámbrico. Cada protocolo especifica varios aspectos de transferencia de datos que los distingue de las otras certificaciones.

4.5.3 CSMA/CD

Uno de los más populares estándares puestos por el grupo 802 fue el estándar 802.3. Esta es la certificación usada por dispositivos Ethernet. Por ejemplo un dispositivo debe soportar una tecnología conocida como "Acceso Múltiple por Detección de portadora/Detección de colisión" (CSMA/CD). Analicemos por partes esta tecnología, Detección de portadora, que básicamente significa que solo una persona (o dispositivo) puede hablar al mismo tiempo, imaginemos la confusión presente si todos quieren hablar al mismo tiempo. La siguiente parte seria Acceso múltiple, el cual es una forma técnica de decir que hay mas de una persona (o dispositivo) escuchando la conversación. Ejemplo, en una clase, todos escuchan las palabras dichas por un instructor a un estudiante. Sin embargo si el instructor esta hablando a un estudiante en especifico, la información la información que esta siendo pasada es irrelevante para los otros y puede ser ignorada por el resto de la clase. Lo mismo aplica a las redes Ethernet. La última parte es detección de colisiones, lo cual es otra forma de decir que cada dispositivo Ethernet puede determinar cuando dos dispositivos han iniciado hablando al mismo tiempo. Cuando los humanos hacemos esto, nosotros simplemente paramos y entonces una persona empieza a hablar otra vez. En un ambiente Ethernet, los dispositivos pararan y esperaran una cantidad de tiempo aleatorio. El dispositivo que tiene el tiempo aleatorio mas bajo empezara a hablar primero.

4.5.4 CSMA/CA

Las redes 802.11 usan CSMA/CA o CSMA/evasión de colisiones que es una alternativa a CSMA/CD. Hace esto enviando un mensaje de Broadcasting con la intención de hablar. En otras palabras esto es como llamando la pelota cuando jugamos volleyball. Si todos saben quien intenta ir por la pelota, las personas no trataran de correr hacia los otros tratando de regresar la pelota. Sin embargo este tipo de comunicación no tiene algo de encabezados extras, como que cada dispositivo de red debe enviar sus datos de salida sobre la red antes de empezar a transmitir. Aunque la parte individual de datos es pequeña, la cantidad acumulativa

puede volverse excesivo en una red sobrecargada. 802.11 no es el único estándar que usa CA de hecho Appletalk, usado por las computadoras Mac, también usa CA en su red de datos.

802.11 es una serie de estándares que define los métodos de transmisión inalámbricos de trafico Ethernet. Comúnmente referido como Wi-Fi o tráfico WLAN, esta tecnología es probada y comercializada por la WECA (Wireless Ethernet Compatibility Alliance).

Este estándar tiene algunos sub-estándares importantes para entender las WLANs 802.11a, 802.11b y 802.11g. Cada uno de estos esta basado en diferentes capas físicas y tiene sus propios beneficios y desventajas.

4.5.5 Pre-estándar

Algunas otras tecnologías fueron desarrolladas que usaron varias formas de salto de frecuencia, para facilitar la transferencia de datos inalámbricos. Estas tecnologías eran propietarias y eran típicamente lentas en relación al estándar terminado, con velocidades de 1-2 Mbps y frecuencias de 900 MHz y 2.4 GHz. Todos los estándares 802.11x usan la banda de frecuencia ISM (Industria, ciencia y medicina).

Después que el estándar 802.11 fue ratificado en 1997, tres principales tecnologías de fueron los métodos de transmisión de datos: DSSS, FHSS y IrDA. De los tres DSSS y FHSS, mostraron mas promesas, y fueron eventualmente incorporados dentro de la mayoría de las tecnologías WLAN.

4.5.6 El estándar 802.11

El estándar 802.11 define los protocolos que gobiernan todo el tráfico inalámbrico basado en Ethernet. Además dentro de este estándar existente algunos sub-estándares que competente con cada uno de los otros por un lugar en el mercado.

En las propuestas de estándares inalámbricos para LAN del IEEE (IEEE 802.11), hay dos diferentes maneras de configurar una red:

1. Ad-hoc
2. Infraestructura.

En las redes ad-hoc, las computadoras son unidas entre ellas mismas para formar una red "en el aire", no hay infraestructura hacia la red alambrada, no hay puntos de acceso, y usualmente cualquier nodo es capaz de comunicarse con cualquier otro nodo. Un buen ejemplo de esto es cuando los empleados traen computadoras portátiles, para comunicarse y compartir información de diseño o financiera. Aunque esto parece que el orden debería ser difícil de mantener en este tipo de red, algoritmos tales como el algoritmo de elección de vocero (SEA) ha sido diseñado para seleccionar una maquina como la estación base (maestra) de la red con los otros siendo esclavos.

Otros algoritmos en redes de arquitectura ad-hoc usan métodos de difusión e inundación para todos los nodos, para establecer quien es quien.

El segundo tipo de estructura de red usado en LAN inalámbricas, es la infraestructura. Esta arquitectura usa puntos de accesos fijos de red, son algunas veces conectados a líneas de cable para ampliar la capacidad de las LAN cuenteando nodos inalámbricos a otros nodos de alambre. Si área de servicio se traslapan, puede ocurrir el handoffs. Esta estructura es muy similar a las redes celulares que hoy existen alrededor del mundo.

Una LAN 802.11 es basada en la arquitectura celular donde el sistema es subdividido en celdas, donde cada celda es llamada BSS (Basic Service Set en la nomenclatura de 802.11) es controlada por una estación base (llamada Access Point o AP)

Pensando que una LAN inalámbrica puede ser formada por una celda simple, con un access point, muchas instalaciones serán formadas por algunas celdas, donde el

access point es conectado a través de alguna clase de backbone (llamado sistema distribuido o DS) típicamente Ethernet, y en algunos casos el mismo inalámbrico.

El total de las LAN inalámbricas interconectadas incluyen las diferentes celdas, sus respectivos access point y el sistema de distribución, es visto el capas superiores del modelo OSI, como una red 802 simple y es llamada en el estándar como ESS (extended Service Set).

El estándar también define el concepto de portal, un portal es un dispositivo que interconecta una 802.11 y otra LAN 802.

4.5.7 Banda de frecuencia 2.4 GHz.

La banda de frecuencia 2.4 GHz., es una banda abierta en la cual muchos dispositivos operan, incluyendo teléfonos y hornos de microondas la FCC abrió esta banda de frecuencia para permitir a los vendedores crear dispositivos inalámbricos que no requieran de aprobación especifica de la FCC. En otras palabras, cualquiera puede hacer dispositivos en la banda de 2.4 GHz. y usarlos sin estar sujeto a regulaciones de frecuencia (pagos por uso del espectro electromagnético).

4.5.8 Banda de frecuencia 5 GHz.

La banda de frecuencia de 2.4 GHz. esta muy saturada por muchos dispositivos, sin embargo, el rango de frecuencia de 5 GHz. todavía libre de este problema. En adición la banda de 5 GHz., significa mas transferencia de datos en el mismo tiempo, si comparamos 2.4 GHz. contra 5 GHz., vemos que hay una diferencia del doble de rápido, en combinación con diferentes técnicas de control de frecuencia, hacen al 802.11a cinco veces mas rápida que su predecesor el estándar 802.11b.

4.5.9 DSSS

DSSS es un método de envió de datos en el cual es transmisor y el receptor están puestos en un ancho de frecuencia de 22 MHz. El canal amplio permite a los

dispositivos transmitir más información en comparación con un sistema de FHSS. DSSS combina los datos de una señal que son enviados por una estación con una secuencia de bit de alta velocidad, la cual es referida como ganancia de procesamiento. Una alta ganancia de procesamiento incrementa la resistencia de la señal a las interferencias. La ganancia de procesamiento para los dispositivos 802.11 requiere un valor mínimo de 11.

DSSS (secuencia directa/ espectro disperso), ayuda a prevenir interferencia a través del uso de la dispersión de la señal sobre algún rango de frecuencia en un tiempo.

4.5.10 FHSS

FHSS (Frecuency hopping/spread spectrum), usado en la banda de 2.4 GHz., una señal puede cambiar la frecuencia de la portadora o salta, acorde a una secuencia seudo-aleatoria. La secuencia seudo aleatoria es una lista de algunas frecuencias en las cuales la portadora podrá saltar en periodos de tiempo específicos antes de que repita la lista nuevamente.

Usando el rango de frecuencia entero, múltiples redes pueden operar en la misma área sin temor a colisiones. FHSS es usado en redes denominadas HomeRF y el primer estándar de las WLAN (802.11).

4.5.11 OFDM (Múltiplex por división de frecuencia ortogonal)

Es un esquema de transmisión que como todos los esquemas de transmisión, codifican datos dentro de una señal de radio frecuencia. Esquemas de transmisión convencional de portadora simple como AM/FM (modulación por amplitud o frecuencia) envían solo una señal en un tiempo sobre una frecuencia de radio, mientas de OFDM envía una señal de alta velocidad al mismo tiempo en diferente frecuencia. Esto permite uso muy eficiente del ancho de banda y proporciona comunicación robusta en el momento de ocurrencia de ruido.

4.5.12 Opciones de transmisión

Hay básicamente tres tecnologías de RF, microondas de banda angosta, espectro disperso y OFDM:

En banda angosta, la potencia para transmitir los datos es incrementada para vencer el ruido. Esto mejora el rendimiento de las transmisiones, pero interfiere con otras señales que están siendo enviadas por otros usuarios en la banda, causando errores en los datos de los otros. Los sistemas de banda angosta son también sensitivos a interferencia multi-ruta, en el cual nuestra propia señal es reflejada en un objeto y llega tarde a su destino con respecto a la señal original, esto hace que la señal original y la reflejada se "pelen" por ser atendidos por su receptor, esto requiere continuamente ajustar y sintonizar utilizando hardware lo cual significa un incremento del costo del sistema.

Las tecnologías de espectro disperso usa mucho más ancho de banda que el requerido para vencer el ruido y problemas de multi-trayectoria. Desafortunadamente como se incrementa la cantidad de datos, así es requerido el ancho de banda. Los mejores sistemas para entregar 11 Mbps usan 22 MHz del espectro.

Las tecnologías de OFDM rompen una señal de datos de alta velocidad en decenas o cientos de señales de baja velocidad, las cuales son transmitidas en paralelo. Esto crea un sistema altamente tolerante al ruido y a las multi-trayectorias y al mismo tiempo es muy eficiente en el uso del ancho de banda. La inmunidad al ruido y a la multi-trayectoria permiten para áreas amplias, cobertura multipunto y el uso eficiente del ancho de banda permite muchos mas canales de alta velocidad dentro de una banda de frecuencia. Por lo tanto las tres dificultades en banda angosta y espectro disperso son vencidas por OFDM.

4.5.13 Las ventajas de OFDM

Eficiencia espectral, el cual traslada más bps/Hz. que los esquemas de transmisión convencional.

La eficiencia espectral es adicionalmente aumentada como el espectro puede ser hecha para verse como una ventana rectangular, significando que todas las frecuencias son utilizadas similarmente.

OFDM es menos sensitivo a errores de temporización, los errores de temporización es simplemente trasladado a un offset de fase en el dominio de la frecuencia. Los esquemas de transmisión OFDM, son una versión óptima de los esquemas de transmisión multi-portadora. El concepto de uso de transmisión de datos paralelos y multiplexión de frecuencia fue publicada a mediados de los años 60´s. Después de más de 30 años de investigación y desarrollo, OFDM ha sido ampliamente implementado en comunicaciones digital de alta velocidad. Debido a los recientes avances en el procesamiento de señal digital (DSP) y tecnologías de circuitos integrados de alta escala de integración (VLSI).

El uso de algoritmos de la transformada rápida de Fourier elimina arreglos de generadores senoidales y modulación coherente requerida en sistemas de datos paralelos.

El concepto de OFDM es basado en la dispersión de datos a ser transmitidas sobre un amplio número de portadoras, cada una modulada a baja velocidad. Las portadoras son hechas ortogonales a cada una de las otras a través de la selección apropiada del espacio de frecuencia entre ellas.

En contraste a la multiplexión de división de frecuencia convencional, el traslape espectral entre sub-portadoras es permitido en OFDM desde que la ortogonalidad asegurara la separación de las sub-portadoras en el receptor, proporcionando mejor eficiencia espectral y el uso de filtros pasa banda por paso fue eliminado.

Los sistemas de transmisión OFDM ofrecen la posibilidad de aliviar muchos de los problemas encontrados con sistemas portadores simples.

Los sistemas de transmisión de OFDM, ofrecen la posibilidad de aliviar muchos de los problemas encontrados en sistemas de portadora simple. Tiene la ventaja de dispersar el desvanecimiento de una frecuencia selectiva sobre muchos símbolos, esto efectivamente aleatoria los errores de ráfaga causados por desvanecimientos o por impulsos de interferencia, así esto en cambio de algunos símbolos adyacentes sean completamente destruidos, muchos símbolos son solo ligeramente destruidos esto permite la reconstrucción exitosa de la mayoría de ellos sin la corrección de errores hace adelante. Debido a la división de un ancho de banda de señal entera en muchas sub-bandas, la respuesta a la frecuencia sobre sub-bandas individuales, es relativamente plano debido a que las sub-bandas son pequeñas en relación al ancho de banda coherente del canal.

La ortogonalidad de los sub-canales en OFDM puede ser mantenida y los sub-canales pueden ser separados completamente por la FFT en el receptor cuando no hay interferencia Inter.-símbolo (ISI) e interferencia Inter.-portadora (ICI) introducida por la distorsión del canal transmitido.

A través del uso de diversidad de tiempo y frecuencia, OFDM proporciona un medio para transmitir datos en canal de frecuencia selectiva. Sin embargo no suprime los desvanecimientos el mismo. Dependiendo de su posición en el dominio de la frecuencia, sub-canales individuales pueden ser afectados por los desvanecimientos. Esto requiere el uso de codificación del canal para adicionar protección a la transmisión de datos

4.5.14 802.11

La IEEE desarrollo el estándar 802.11 para redes de área local inalámbricas (WLAN). Hay cuatro especificaciones incluyendo 802.11, 802.11a, 802.11b y 802.11g. Cada estándar 802.11 opera en diferente rango de frecuencia y/o ofrece

diferentes velocidades de transmisión. 802.11 aplica para LAN inalámbricas y proporcionan transmisión de 1 a 2 Mbps en la banda de 2.4 GHz usando cualquier de las siguientes técnicas: salto de frecuencia/espectro disperso (FHSS) o secuencia directa/espectro disperso (DSSS).

4.5.15 802.11a

La especificación 802.11a opera en el rango sin licencia de 5 GHz y ofrece velocidades de transmisión de datos de hasta 54 Mbps. El rango de 5 GHz no esta saturado y ofrece la ventaja de velocidad por arriba del estándar 802.11b, especificación que usa el rango mas saturado de 2.4 GHz (que puede interferir con teléfonos inalámbricos, microondas, etc.), sin embargo el rango y la velocidad de 802.11a son inversamente relacionados, lo cual es porque el 802.11a no fue adoptado como el estándar de Wi-Fi. 802.11a usa un esquema de modulación de conocido como OFDM (Multiplexión por división de frecuencia ortogonal) contra el FHSS o DSSS. La mayoría de los productos 802.11a no son compatibles con productos 802.11b o 802.11g, aunque esto esta cambiando.

4.5.16 802.11b

El estándar 802.11b opera en el rango de 2.4 GHz y ofrece velocidades de transmisión de datos de hasta 11 Mbps. 802.11b es de hecho el estándar para los servicios Wi-Fi debido a su disponibilidad y bajo precio (aunque 802.11g será dentro de poco el estándar). Mientras sea lento en relación al 802.11a, el 802.11b es todavía rápido como lo es los servicios del Ethernet 10baset. El 802.11b usa secuencia directa/espectro disperso y modulación de keying de código complementario (CCK). 802.11b fue certificada por la IEEE en 1999.

4.5.17 802.11g

El 802.11g fue aprobado el 11 de Junio de 2003 y ofrece velocidades de transferencia de datos de hasta 54 Mbps y opera en la banda de 2.4 GHz. y 5 GHz., haciéndolo compatible hacia atrás con el estándar 802.11b. Antes de que fuera

aprobado por la IEEE, era claro que el 802.11g podría ser el estándar para los servicios de Wi-Fi, y los fabricantes líderes, empezaron a liberar productos en los inicios del 2003. 802.11g usa modulación OFDM pero, para hacerlo compatible hacía atrás con 802.11b, soporta también modulación por switcheo de código complementario (CCK).

Con toda la corriente de estándares 802.11, hay una cuestión acerca de la seguridad, velocidad, rango, interferencia y el precio. Actualmente están en proceso estándares como el 802.11e que incluye calidad de servicio, 802.11n el cual incrementa la velocidad de transmisión de datos hasta más de 100 Mbps (108 Mbps) y el estándar 802.11i el cual incluye mejoras en la seguridad con respecto a los actuales estándares. Además de esto se piensa en un estándar llamado WiMax para redes WAN inalámbricas. Seria interesante ver si la industria tiene la intención de fabricar dispositivos con los nuevos estándares en un solo dispositivo.

El destino de las redes inalámbricas 802.11 esta asegurado dado la actual demanda de equipo reflejado por las altas ventas y las altas inversiones que los fabricantes invierten en esta tecnología, así mismo tal parece que los organismos trabajan constantemente en el desarrollo de estándares que constantemente mejoran el rendimiento y seguridad de los dispositivos WLAN. No seria exagerado pensar que las redes inalámbricas dominen una parte considerable amplia del mercado de tecnologías de red.

4.6 Comparativas de tecnologías

En 1999, la IEEE define dos adiciones a la capa física del 802.11, llamada 802.11b y 802.11a. 802.11b adiciona velocidades de datos de 5.5 y 11 Mbps (para solo DSSS) y básicamente extiende las capacidades de 802.11. Por el otro lado, 802.11a introduce enteramente nuevas capacidades para soportar altas velocidades de transmisión. Mientras que el estándar 802.11g fue recién aprobado en el año de 2003.

Desde este tiempo, 802.11b ha sido probado por ser enormemente exitoso. Numerosos productos basados en el 802.11b han sido introducidos al mercado y una organización devota de la interoperatividad de estos productos ha sido establecida. Esta es la organización llamada WECA (Alianza de Compatibilidad Ethernet Inalámbrica). Es la responsable de otorgar el logo de Wi-Fi (Wireless Fidelity) a los productos que cumplen con los requerimientos de interoperatividad. Aunque el 802.11b y Wi-Fi no son estrictamente sinónimos, todas las pruebas de WECA están soportadas firmemente en el estándar 802.11.

Productos basados en el 802.11a empezaron a emerger a finales del 2001. WECA iniciaría su programa de logo Wi-Fi5 una vez que al menos dos compañías de semiconductores produzcan circuitos integrados 801.1a, y fabricantes de equipos, al menos produzcan tres tipos de equipos esto se esperaba ocurriera para mediados del 2002. Los productos 802.11g estuvieron disponibles incluso antes de ser aprobado el estándar, pero solo algunos son ahora compatibles con el estándar 802.11g aprobado, los equipos diseñados antes de la aprobación del 802.11g, estaban basados en el borrador del estándar 802.11g (802.11g draft).

Bandas de frecuencia, operación

802.11b y 802.11g operan en la banda de 2.4 GHz, banda ISM (Industria, Científica y Medica).

802.11a opera en la banda de 5 GHz UNII (Infraestructura de Información Nacional sin licencia).

Operación del ancho de banda

802.11b y 802.11g ocupa 83.5 MHz (para Norte América) desde 2.4000 GHz hasta 2.4835 GHz.

802.11a ocupa 300 MHz en tres diferentes anchos de banda de 100 mhz cada uno:

12. 1. 5.150 a 5.250 GHz (U-NII banda baja)
13. 2. 5.250 a 5.350 GHz (U-NII banda media)
14. 3. 5.725 a 5.825 GHz (U-NII banda alta)

4.6.1 Numero de canales

802.11b y 802.11g proporciona 11 canales (para Norte América), cada canal siendo de 22 mhz de ancho, y cada canal centrado a intervalos de 5 mhz (empezando en 2.412 ghz y terminando en 2.462 ghz). Esto significa que hay solo tres canales que no se traslapan (canales 1, 6 y 11).

802.11a proporciona 12 canales, cada canal siendo de 20 mhz de ancho, y cada uno centrado a intervalos de 20 mhz (empezando en 5.180 ghz y terminando en 5.320 ghz para las bandas baja y media de U-NII, empezando en 5.745 ghz y terminando en 5.805 ghz para la banda alta de U-NII. Es importante notar que ninguno de estos canales se traslapa.

Estandar inalambrico	802.11b	802.11a	802.11g
Velocidades	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36 48 y 54 Mbps	1, 2, 5.5, 11, 6, 9 12, 18, 24, 36, 48 y 54 Mbps
Frecuencia	2.4 GHz	5 GHz	2.4 GHz
Rango	De 30 a 50 metros en interiores	De 8 a 25 metros en interiores	De 30 a 50 metros en interiores
Compatibilidad	Adoptado ampliamente	Incompatible con 802.11b y 802.11g	Compatible con 802.11b a 11 Mbps incompatible con 802.11a
Canales no traslapados	3	24	3
Tecnicas de modulacion	BPSK, QPSK	BPSK, QPSK QAM	BPSK, QPSK QAM, CCK
Medio inalambrico	DSSS	OFDM	OFDM
Costo	Relativamente barato	El mas caro de los tres estandares	ligeramente mas caro que el 802.11b

Figura 4.6.1-1 Comparativa WLAN

Desde que ambos 802.11b y 802.11 segmentaron el ancho de banda disponible en canales, ambos caen dentro de la categoría general de sistemas FDMA (Acceso múltiple por división de frecuencia). Esto no debe ser confundido con OFDM (multiplexión por división de frecuencia ortogonal) como es usado por el 802.11a en su capa física.

4.6.2 Canales de acceso

Todos los estándares 802.11a, 802.11b y 802.11g usan la capa MAC del estándar original 802.11 y ambos usan CSMA/CA para escuchar antes de transmitir en un canal dado. Adicionalmente ambos usan CCA (Valoración de canal libre) para decidir si un canal no esta usado (desde la perspectiva de la calidad de la señal opuesto a la perspectiva de ocupación del canal).

4.6.3 Potencia de transmisión

El 802.11b permite una máxima salida de potencia de 1000 mW, sin embargo la mayoría de los productos son diseñados para salida de no más de 30 mW por razones de disipación térmica y consumo de energía eléctrica (incluyendo duración de la batería para aplicaciones móviles).

802.11a proporciona diferentes salidas de potencia para cada banda de U-NII:

40 mW (banda baja de U-NII)

200 mW (banda media de U-NII)

800 mW (banda alta de U-NII)

La banda baja es aplicad para aplicaciones interiores mientras que la banda alta es aplicada para aplicaciones exteriores

Velocidades de transmisión

802.11b soporta transmisor de datos de 1, 2, 5.5 y 11 Mbps

802.11a soporta transmisión de datos a 6, 12 y 24 Mbps de forma obligatoria y de forma opcional 9,18, 36, y 54 Mbps.

4.6.4 Técnicas de portadora simple y multi portadora.

802.11b usa DSSS (espectro disperso de secuencia directa) con una portadora simple por canal.

802.11a usa OFDM (multiplexión por división de frecuencia octogonal) con multi-portadora (sub-portadoras) por canal.

802.11g utiliza OFDM en la banda de 2.4 GHz.

La teoría básica de comunicación establece que si dos sistemas de radio transmiten en el mismo nivel de potencia y utilizan el mismo esquema de codificación, si se traslada un sistema de al banda de 2.4 GHz a 5 GHz el rango de cobertura se ve disminuido este es el caso de sistemas 802.11b y 802.11g contra el 802.11a en la banda de 5 GHz. Sin embargo para dos sistemas uno 802.11b y otro 802.11g a la misma distancia, el rendimiento es superior dado las diferencias en las técnicas de modulación.

Los sistemas basados en 802.11b utilizan técnicas de modulación que son más simple en relación a las técnicas de modulación utilizadas por 802.11g (DBPSK y DQPSK contra QAM 16 y QAM 64), además de que estas técnicas de modulación utilizadas en 802.11b trasportan menos datos que las técnicas de modulación del estándar 802.11g.

4.6.5 Co-existencia con otros dispositivos inalámbricos

Debido a que el estándar trabaja en una banda de frecuencia (5 GHz) donde no operan otros dispositivos inalámbricos como teléfonos inalámbricos, hornos de microondas, dispositivos bluetooth u homero, etc., es muy raro que las redes 802.11a sean victimas de interferencia por otros dispositivos que no sean WLAN en 802.11a.

Capitulo 5 Infraestructura WLAN

5.1 Infraestructura WLAN

Hay muchos fabricantes de dispositivos de puntos de acceso (access point) y la mayoría de ellos desarrollan las mismas funciones, sin embargo hay muchas diferencias sustanciales en seguridad y características entre los vendedores de equipo. Por ejemplo algunos puntos de acceso son capaces de restringir la conexión a usuarios basados en la dirección MAC de la tarjeta de red inalámbrica, mientras que otros tiene la capacidad de apagar la señalización de guía broadcast, haciendo de esta manera invisible el punto de acceso para los hacker. Afortunadamente características avanzadas en seguridad tales como estas están siendo más comunes en SOHO (small office/home office).

5.1.1 Puntos de acceso (access point)

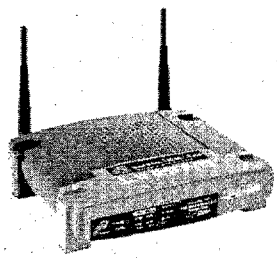


Figura 5.1.1-1 Access point

Existen puntos de acceso los cuales disponen de conexión Ethernet para poder conectar a la red alambrada, estos dispositivos por si solos funcionan como un hub pero inalámbrico donde varias computadoras con tarjeta de red inalámbrica, pueden conectarse la comunicarse entre ellas o para conectarse a la red Ethernet alambrada a la cual este conectada el dispositivo punto de acceso.

Los puntos de acceso se comunican con sus clientes inalámbricos, con la red por cable y con otros puntos de acceso. Hay tres modalidades en las que un punto de acceso puede ser configurado:

Modo raíz

Modo repetidor

Modo puente

Los cuales se describen a continuación

5.1.2 Modo raíz

El modo raíz es usado cuando un punto de acceso es conectado a una red por cable a través de una interfaz Ethernet. La mayoría de los puntos de acceso que soportan diferentes tipos de modalidades, vienen configurados en la modalidad de raíz por default. Cuando un punto de acceso esta en la modalidad de raíz, el punto de acceso es conectado al sistema de distribución por cable entonces puede comunicarse con otros sobre el mismo segmento alambrado.

Los puntos de acceso hablan a otros para coordinar las funciones de Roaming tales como reasociación. Los clientes inalámbricos pueden comunicarse con otros clientes inalámbricos que están ubicados en diferentes células, a través de sus respectivos puntos de acceso cruzando el segmento alambrado de la red.

5.1.3 Modo puente.

En el modo puente, un punto de acceso actúa igual a un puente inalámbrico, y proporciona conectividad entre dos segmentos de red LAN por cable y es usado en configuración punto a punto o punto a multi-punto. Solo algunos dispositivos en el mercado tiene la capacidad de puenteo, que típicamente adiciona un costo extra al producto.

5.1.4 Modo repetidor

En el modo repetidor, un punto de acceso tiene la habilidad de proporcionar un flujo de enlace inalámbrico. Esto debido a que a través de el se conectan varios clientes. El punto de acceso en modo repetidor se conecta inalámbricamente hacia un punto de acceso configurado en la modalidad de raíz. El punto de acceso en modo repetidor se conecta a sus clientes como un punto de acceso y se conecta hacia el punto de acceso en modo raíz, como un cliente del mismo. Usuarios conectados al punto de acceso en modo repetidor experimentaran bajas velocidades de transmisión y altos retardos (latencias) relacionadas con la configuración del sistema mismo.

Un punto de acceso es considerado un portal debido a que permite a sus clientes conectividad desde una red 802.11 hacia una red 802.3 o 802.5. Los puntos de acceso están disponibles con muchas opciones diferentes de hardware y software. Los más comunes son:

Antenas fijas o desmontables.

Capacidades de filtrado avanzado

Tarjetas de radio removibles (modulares)

Salida de potencia variable

Distintos tipos de conectividad a redes por cable

Antenas fijas o desmontables

Dependiendo de las necesidades de la organización o de los clientes, deberemos seleccionar entre un punto de acceso con antenas fijas o removibles. Un punto de acceso con antenas removibles da la habilidad de acoplar una antena diferente a las originales, permitiendo esto instalar antenas omnidireccionales o antenas direccionales según sea la necesidad, también permite poner las antenas a una

distancia considerable dependiendo de la longitud del cable que se utilice, permitiendo de esta forma instalar las antenas en el exterior mientras que el punto de acceso se mantiene en el interior. Los puntos de acceso pueden comprarse con o sin diversidad de antena

5.1.5 Capacidades de filtrado avanzado

Funciones de filtros de protocolo, MAC e IP pueden ser incluidas en los puntos de acceso. Proporcionan protección básica a la red inalámbrica, pueden configurarse listas de acceso que permitan el acceso solo a los dispositivos listados en estas (MAC o IP) incluso listas de bloqueo de protocolos (HTTP, SMTP, FTP, ETC.)

5.1.6 Tarjetas de radio removibles

Algunos fabricantes adicionar o remover una tarjeta de radio desde algún slot (ranura) PCMCIA en el punto de acceso, algunos disponen de hasta dos tarjetas de radio PCMCIA, permitiendo a una de estas actuar como punto de acceso, mientras que la otra actúa como puente. En otros casos cada tarjeta actúa como un punto de acceso independiente uno del otro, esto incrementa el ancho de banda disponible para los usuarios inalámbricos, pudiendo acomodar más usuarios inalámbricos en el mismo espacio físico.

5.1.7 Salida de potencia variable

El control de la salida de la potencia, permite a los administradores controlar la potencia (en mili-watts) que el punto de acceso usa para enviar sus datos. El control de la salida de la potencia puede ser necesario en algunas situaciones donde un nodo distante no puede localizar el punto de acceso, esto también ayuda en la seguridad, permitiendo controlar el tamaño apropiado de la célula y así evitar que algún intruso pueda conectarse a la red desde afuera de las instalaciones de la empresa. La otra alternativa es hacer uso de amplificadores, atenuadores o antenas de alta ganancia para variar la salida de la potencia.

5.1.8 Distintos tipos de conectividad a redes por cable

Las distintas opciones de conectividad en el punto de acceso pueden incluir 10baseTx, 10/100baseTx, 100baseFx y otros. Debido a que un punto de acceso es típicamente un dispositivo a través del cual los clientes se comunican a la red por cable, el administrador debe de saber cual es el medio mas adecuado para conectar el punto de acceso a la red por cable, considerando las características propias de cada una de las tecnologías, nos permitirán determinar cual es el mas adecuado para cada situación.

5.1.9 Router access point

Este es un router que tiene además las funciones de punto de acceso inalámbrico, al tener el router directamente conectado al punto de acceso, podemos compartir nuestra conexión de Internet directamente a usuarios inalámbricos o a usuarios de la red alambrada, algunos router tiene internamente un Firewall con funciones básicas, lo único que necesitamos es una conexión a Internet con su respectivo bridge que nos permita la conexión al ISP (proveedor de servicio de Internet). Incluso algunos

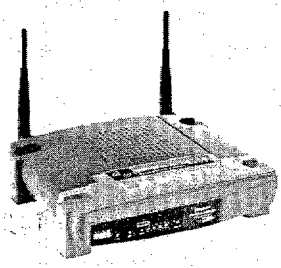


Figura 5.1.9-1 Router access point

router access point tienen la capacidad de realizar conexiones VPN para conectar usuarios remotos a través de este medio.

5.1.10 Tarjetas de red inalámbricas

Existen tarjetas de red inalámbricas para computadoras con interfaces como Cardbus para ser usadas en computadoras portátiles, interfaz PCI para ser instaladas en computadoras de escritorio, en el caso de la tarjeta de red inalámbrica para computadora portátil, antena viene inter construida en la misma tarjeta, para el caso de la tarjeta de red inalámbrica PCI, esta tiene una antena que se puede desmontar o instalar a través de un conector del tipo SMA, lo que permite instalar una antena de mayor ganancia y/o una antena exterior.

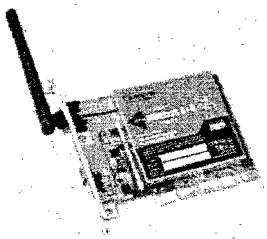


Figura 5.1.10-1 Tarjeta de red WLAN PCI

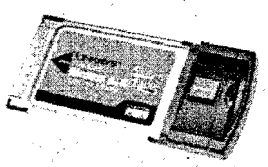


Figura 5.1.10-2 Tarjeta de red WLAN Cardbus

5.1.11 Servidores de impresión

Los servidores de impresión son dispositivos que permiten compartir impresoras en entornos de red sin la necesidad de que esta este conectada a una computadora y esta este encendida permanentemente, por lo regular la interfaz que va hacia la impresora es una interfaz USB 1.1 o 2.0, la versión depende del fabricante de equipo, en el caso de los servidores de impresión inalámbricos la interfaz que

permite conectarse a la red es un dispositivo Wireless, para el caso de los servidores de impresión la mayoría son dispositivos Ethernet que permiten conexión a la red local y puertos paralelos que son conectados a/las impresoras.

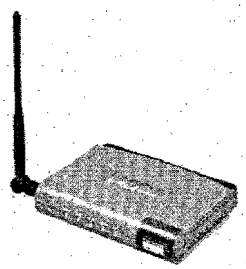


Figura 5.1.11-1 Servidor de impresión

5.1.12 Adaptadores USB

Estos pueden ser considerados dispositivos de red con conexión USB hacia la computadora portátil o hacia la computadora de red. Esta modalidad permite la versatilidad de poder usar un dispositivo de este tipo con equipo portátil o de escritorio, y al igual que cualquier dispositivo USB pueden ser conectados y desconectados en cualquier momento a una computadora.

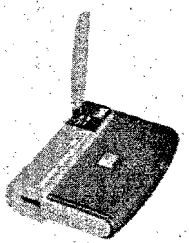


Figura 5.1.12-1 Adaptador USB

5.1.13 Ethernet bridge

Dispositivos para puentes un equipo con tarjeta de red Ethernet por cable hacia un red inalámbrica, incluso puede conectarse en un hub o switch para puentear toda la red. Si se dispone de dos rede por cable, mediante el uso de un bridge inalámbrico, podemos conectar un segmento de la red al el segmento de la red principal sin el uso de cables de par trenzado o fibra óptica, reduciendo los costos de instalación del cable. Pueden configurarse para ser usados en conexiones punto a punto (modo bridge), punto a multi-punto (modo no raíz) o como repetidores entre dos segmentos de red con conexión inalámbrica cada una.

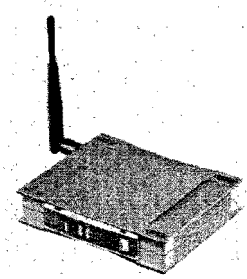


Figura 5.1.13-1 Wireless Ethernet Bridge

5.1.14 Tarjeta de red inalámbrica para PDA

Los dispositivos PDA pueden también conectarse a redes inalámbricas a través de tarjetas de red inalámbricas con interfaces compact Flash. Para los distintos dispositivos de interconexión existen en diferentes estándares como son: 802.11a, 802.11b y 802.11g, cada uno de los cuales tiene sus características muy particulares. Algunos dispositivos vienen con doble estándar o incluso triple, los dispositivos 802.11b que fueron los primeros en salir en forma masiva solo disponen de este estándar, los dispositivos con estándar 802.11g también traen en la mayoría de los casos estándar 802.11 y hay dispositivos con el estándar 802.11a y el estándar 802.11g.

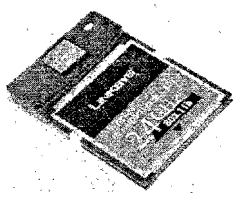


Figura 5.1.14-1 Wireless para PDA

5.1.15 Cámaras de video

Las cámaras de video han incrementado su uso debido a condiciones de inseguridad, las cámaras permiten incrementar el área que se quiere asegurar, por esta razón ahora las cámaras de video de circuito cerrado ahora pueden ser usadas en ambientes de red alambrada, Ethernet a 10/100 Mbps e incluso sobre una red inalámbrica bajo estándares como el 802.11b. La ventaja de la cámara inalámbrica es la facilidad de instalación sin depender de una instalación previa para su uso, solo se requiere montarle en un buen lugar y aplicarle energía.

Figura 5.1.15-1 Cámara de video inalámbrica

No requiere de conexiones a una red inalámbrica o conexiones de cable coaxial para CCTV. Actualmente hay cámaras en varios estándares como el 802.11b y 802.11g, algunas además de ser inalámbricas también cuentan con conexión de red Ethernet.

5.1.16 Adaptador de medios de audio y video inalámbrico

Los adaptadores de medios de audio e imágenes son equipos inalámbricos que permiten escuchar el audio de un archivo dentro de una computadora en un equipo de sonido, también permiten ver imágenes almacenadas en una computadora, y ser vistas en una televisión. Para el sonido, los adaptadores cuentan con salidas estándar de audio de canal izquierdo y derecho tipo RCA, los cuales son conectados a través de un par de cables a un equipo de sonido.

Para el video los adaptadores de medios, cuentan con salidas de video estándar tipo RCA y con salida de video S, los cuales pueden ser conectados con cables a una televisión normal. Las aplicaciones de estos dispositivos son prácticamente para el hogar, con centros de entretenimiento. Logrando escuchar música en formatos como MP3 y WMA, y ver archivos de imágenes como JPG y BMP entre otros. No es necesario una concesión física entre en equipo que tiene los archivos multimedia y el centro de entretenimiento, todo viaja a través de la conexión inalámbrica.

5.1.17 Dispositivo inalámbrico de presentación

Los dispositivos inalámbricos de presentaciones, funcionan como un punto de acceso con una conexión para salida de video VGA estándar, donde se puede conectar un monitor o un proyector, cualquier cliente inalámbrico dentro del rango del punto de acceso y con los permisos adecuados puede tomar el control de proyector o monitor. Estos dispositivos son de gran utilidad cuando las presentaciones las realiza más de una persona a la vez, permitiendo a cada expositor, traer su propio equipo y poder conectarse a proyector de forma inalámbrica desde cualquier ubicación en la sala de exposición. Algunos dispositivos cuentan con conexión USB donde se puede conectar una memoria portátil con

conexión USB y en donde se puede almacenar una presentación, la cual puede ser proyectada.

5.1.18 Antenas

Casi la mayoría de las personas usa al menos una antena al día, de hecho si consideramos todos los dispositivos posibles que usen antena, la mayoría usa una al menos para conveniencia de su estilo de vida, por ejemplo al escuchar radio, al ver televisión, al usar el control remoto de la alarma del automóvil, localizadores de persona (pager), telefonía celular, sistemas de televisión satelital y por que no, hasta redes inalámbricas, todas requieren de al menos una antena para su operación.

Las antenas son una extensión del radio transmisor o receptor, como una señal es generada, esta es pasada del radio hacia la antena para ser enviada sobre el aire y recibida por otra antena, entonces pasa al otro radio para su procesamiento. La señal que es generada y después transmitida es medida en Hertz y dBm, donde los Hertz expresan la razón de cambio de la señal portadora (ciclos por segundo), en muchos de los casos expresados en múltiplos, como KHz, MHz y GHz.

Como podemos ver las antenas son fundamentales para los equipos inalámbricos, en general, para la transmisión de radiofrecuencia. En muchos casos se transmite una señal de baja potencia usando una buena antena, la señal puede llegar a su destino con un margen de seguridad aceptable. Las antenas son medidas eléctricamente principalmente por la ganancia que pueden proporcionar. La ganancia de una antena es una medida de la eficiencia de la misma, al medir su potencia radiada en una determinada dirección. Además es la relación de la potencia radiada en una antena con relación a la potencia radiada a una antena de referencia, como la antena isotropita o la antena dipolo, manteniendo la misma constante de potencia que entrega un transmisor.

Una antena dipolo tiene 2.15 dB de ganancia sobre una antena isotropita de 0 dBi, si la ganancia de una antena esta dada en dBd y no en dBi, entonces:

$$0_{dBi} = 2.15_{dBd}$$

Ecuación 5.1.18-1 Relación dBi a dBd

Para una antena con ganancia expresada en dBd

dBi = dBd + 2.15 ó

dBd = dBi –2.15

La mayoría de las antenas que son vendidas expresan su ganancia en dBi, la mayoría de las tarjetas de red inalámbricas transmiten con una potencia de 32 mW, esto es igual 15 dBm.

Por consiguiente si estamos usando una tarjeta de red inalámbrica con 15 dBm de potencia y usamos una antena de 3 dBi de ganancia, podemos calcular la potencia radiada isotropita efectiva (EIRP):

EIRP = Potencia de transmisor + ganancia-perdidas

En este caso suponemos que por el momento no hay pérdidas, entonces:

EIRP = 15 dBm + 3 dBi = 18 dBm (64mW)

En adición a la ganancia de la antena y la potencia del transmisor, debemos también considerar la diferencia en tamaño de las antenas. Dependiendo de la frecuencia y tipo de antena habrá una variedad de tamaños para escoger. El tamaño de la antena esta directamente relacionado con la frecuencia.

Hay dos tipos principales de antenas usados en redes inalámbricas, omnidireccionales y direccionales. Las antenas omnidireccionales pueden recibir y

transmitir desde cualquier extremo alrededor de ella (360 grados). Estas son usadas para proporcionar cobertura general alrededor de esta. Las antenas omnidireccionales solo radian sobre el plano de las X (horizontal) y no en el plano de las Y, esto es un modelo tridimensional, donde un disco con cierto grosor representaría la cobertura real de una antena omnidireccional, el grosor representaría el ángulo de inclinación del patrón de radiación, hacia arriba y hacia debajo de la horizontal.

En particular las antena direccionales toman la energía de RF y la concentran en una dirección especifica, también toma una forma tridimensional, creando un lóbulo en la dirección deseada con ancho en el plano de las X y de las Y, definido por el fabricante. Las antenas direccionales son usadas ampliamente en enlaces punto-punto inalámbricos, o cuando intentamos reducir la señal de RF en una dirección.

5.2 Antenas y accesorios

Los equipos WLAN al igual que cualquier otro dispositivo inalámbrico requieren de accesorios extras para poder radiar la señal electromagnética en el espacio libre, en especial en los puntos de acceso que requieren ser conectadas con antenas externas o tarjetas de red con antenas externas. Cada uno de estos dispositivos o accesorios cumple con un cometido muy particular, por lo cual es importante saber cual de ellos nos puede ayudar a implementar una red inalámbrica y/o resolver algún problema que se nos presente.

5.2.1 Antenas.

Las antenas son un elemento importante en los sistemas de comunicación inalámbrica, son la interfaz entre el radio y el medio de propagación que en este caso es el espacio libre. Existe una amplia variedad de antenas para distintas aplicaciones, es conveniente saber que tipo de aplicación esta manejando el sistema de comunicación para poder elegir adecuadamente las antenas.

Las Antenas emplean el voltaje y la corriente de una línea de transmisión o de los campos E y H que provienen de una guía de ondas para lanzar un frente de onda electromagnético (EM) al vacío o a un medio local. La antena actúa como un transductor que permite igualar la línea de transmisión o guía de ondas al medio que rodea la antena. El proceso de lanzamiento se conoce como radiación. La función de la antena es dirigir la energía en la dirección deseada y lo que es a menudo, es más importante, suprimir la radiación en otras direcciones en las que no se necesita. Esta segunda función de las antenas se considera en primer lugar bajo el concepto de características de directividad.

A menudo se emplea el diagrama de radiación relativa que da las intensidades relativas del campo según las distintas direcciones referidas a la unidad tomada en la dirección de radiación máxima.

5.2.2 Parámetros de antenas.

Las antenas existen en diferentes formas pero además tiene parámetros propios para cada tipo de antena que son importantes conocer para determinar el tipo de antena que se debe utilizar de acuerdo a la aplicación para la cual sean usadas estas, el no conocer adecuadamente los parámetros podría causar problemas de comunicación debido a la incompatibilidad del equipo de RF.

5.2.3 Polarización

La polarización de una antena es la dirección del campo E para una recepción máxima de la antena receptora o la dirección del campo E transmitido por la antena, existen antenas con polarización vertical, horizontal, elíptica o circular. En algunas antenas es posible ajustar el tipo de polarización.

5.2.4 Impedancia característica.

Es un parámetro que depende de la relación longitud/diámetro del conductor y de la frecuencia de trabajo. La Zo de cada punto del conductor es también función de su

distancia al punto de alimentación de la antena, por lo que la misma varía a lo largo de la antena

5.2.5 Frecuencia de operación

Es la banda de frecuencia de operación de la antena, estas bandas de frecuencia corresponden con las recomendaciones de la CCIR o recomendaciones locales en todo el mundo.

5.2.6 Pérdidas por propagación en el espacio libre

Las perdidas en el espacio libre se refieren a las perdidas que se presentan en una señal de RF debido a la dispersión de la señal a lo largo de la trayectoria, para antenas isotrópicas en donde la distancia d es expresado en kilómetros y la frecuencia F es expresada en MHz, se tiene que la perdida en el espacio libre es:

$P_0 = 32.4 + 20Log(d) + 20Log(F)$

5.2.7 Ganancia

La ganancia de una antena es función del tamaño de la antena, y es la medida de la concentración de la densidad de potencia en el frente de onda radiado en una dirección determinada. Se representa en dBi o dBd, y esta definida para una banda de frecuencia muy particular. Por lo regular la ganancia varía dentro de márgenes estrechos de la banda de operación.

5.2.8 Relación frente atrás (front to back)

Se da en decibeles y denota la radiación relativa al lóbulo principal a 180° ± 40° a través de la banda.

5.2.9 Discriminación Polarización cruzada

Expresada en dB es la diferencia entre el pico de lóbulo principal co-polarizado y el máximo cruce de la señal polarizada sobre un ángulo doble de 3 dB

5.2.10 Razón de potencia

La capacidad de manejo de potencia para una antena expresada en Watts. Este parámetro debe tomarse en cuenta, en función de la potencia a ser transmitida a través de ella.

5.2.11 VSWR.

Es la relación del valor máximo al valor mínimo del voltaje en el patrón de la onda estando en las terminales de la antena. Y es producido cuando la impedancia de la antena difiere de la impedancia característica de la línea de transmisión.

5.2.12 Angulo del lóbulo (beam tilt)

Generalmente se refiere al ángulo de inclinación del lóbulo principal en el patrón de elevación arriba y debajo de la elevación de 0 grados en la vertical del lóbulo.

5.2.13 Ancho del lóbulo (beam width)

La medición del ancho de ángulo del lóbulo principal medido en grados entre el punto de media potencia (3 dB abajo del máximo) del el lóbulo mayor en cualquier de los patrones de radiación elevación o azimut.

5.2.14 Tipos de antenas según forma de radiación.

De acuerdo a su patrón de radiación podemos dividir a las antenas básicamente en 3 tipos frecuentemente utilizadas en redes WLAN, la selección de una antena debe ser en función del tipo de comunicación que se requiere para comunicaciones punto a punto se utilizan antenas direccionales en ambos extremos, para comunicaciones

punto multipunto se utiliza una antena omnidireccional o sectorial en el punto de acceso y antenas direccionales en los clientes. Las antenas según su patrón de radiación son las siguientes.

5.2.15 Direccionales.

El haz de la onda electromagnética se concentra en una dirección muy particular. Con un ángulo de abertura lo cual obliga a "apuntar directamente hacia el sitio de recepción.

Figura 5.2.15-1 Antena Direccional

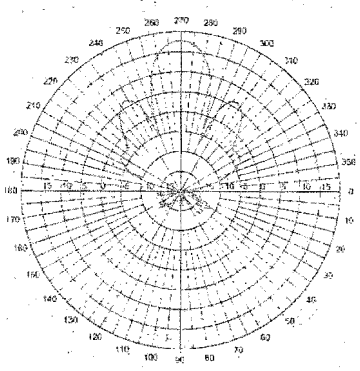


Figura 5.2.15-2 Patrón de radiación direccional

Por lo que este tipo de antena es usado ampliamente para enlace punto-punto ya se satelital, microondas, telefonía rural entre otros.

Dentro de esta misma categoría están, las direccionales de rejillas, tipo corneta (horn), parabólicas, etc. El patrón de radiación es similar a una antena sectorial con la única diferencia de que la direccional tiene un haz mucho mas estrecho que una antena sectorial. (Es más direccional)

5.2.16 Omnidireccionales.

La onda electromagnética es radiada en todas direcciones, en este tipo de antenas el patrón de radiación es similar a un toroide donde la antena se encontraría idealmente en el centro de este. Este tipo de antena es usado ampliamente en sistemas repetidores multipunto tanto el caso de sistemas troncalizados, telefonía rural, telefonía celular, radios convencionales de VHF, UHF, equipo de radiodifusión (Broadcasting), paging, etc.

Figura 5.2.16-1 Antena omnidireccional

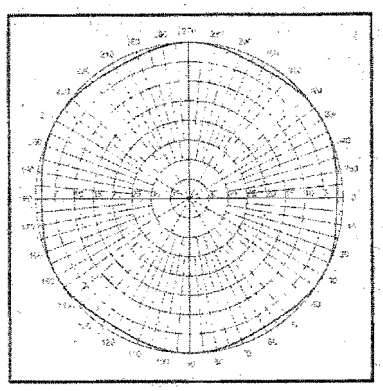


Figura 5.2.16-2 Patrón de radiación omnidireccional

Aunque el patrón de radiación idealmente es en forma de toroide, en forma real tiene un patrón de forma irregular que varia de forma irregular tanto en forma vertical como el horizontal. Aun cuando es una antena omnidireccional debe considerarse que el patrón de radiación en vertical tiene un ancho definido por el fabricante y este parámetro varia de una antena a otro incluso entre el mismo modelo.

5.2.17 Sectorial.

Como su nombre lo indica la radiación electromagnética cubre un sector limitado a no más de 180° o menos, generando sectores de cobertura en función del tipo de antena. Su aplicación es similar al de la antena omnidireccional con la ventaja de solo favorecer a los sectores de área requeridos. Este tipo de antena y las direccionales, incluso se puede mandar a hacer de acuerdo a las necesidades muy particulares de cada punto donde se requiera aplicar. Por ejemplo el ángulo se inclinación del lóbulo principal sobre el horizonte se puede solicitar entre 3 y 7 grados de acuerdo a las inclinaciones de los sitios de terminales con respecto al repetidor que les da cobertura.

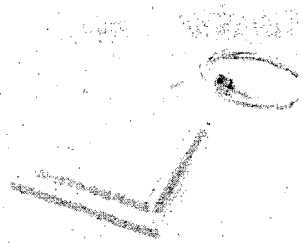


Figura 5.2.17-1 Antena sectorial

También la antenas pueden subdividirse según su aplicación y esto se debe a las bandas de frecuencia de operación del equipo a ser utilizado, la potencia que se maneja en el transmisor, el equipo remoto con el cual se va enlazar la antena en cuestión, las área a cubrir o la distancia del salto entre transmisor local y receptor remoto, el requerimiento del ancho de banda del sistema, el tipo de enlace punto-punto o punto-multipunto.

Existen un sin numero de antenas para distintas aplicación, todas regidas bajo los mismos principio, pero cuyo diseño esta basado en la aplicación para la cual va ser usada, es conveniente conocer nuestras necesidades reales para poder elegir adecuadamente la antena requerida y así evitar sobre-diseñar nuestro sistema elevando los costos de instalación o sub-diseñar y quedarnos cortos en cuanto a nuestras necesidades.

5.2.18 Instalación de antena

Es muy importante tener apropiadamente instalada la antena en una red inalámbrica LAN. Una instalación inapropiada puede dañar el equipo WLAN, además de que puede reducir el desempeño del equipo. Esto es debe haber una buena instalación de las antenas, donde se debe considerar el lugar adecuado para su instalación, el montaje, la orientación y la alineación.

La ubicación de una antena omnidireccional conectada a un punto de acceso debe ser cercana al centro de área de cobertura siempre que sea posible. Ubicar la antena en una punto lo mas alto posible incrementa el área de cobertura, si se usa

antenas de alta ganancia direccionales, se debe tener cuidado de que los usuarios que se encuentren ubicados en la parte trasera de la antena, tengan una recepción adecuada. Las antenas exteriores deben ser montadas arriba de las obstrucciones tales como árboles cables ductos de aire acondicionado y construcciones para que estos no invadan la zona de Fresnel y no creen efectos de multi-trayectoria.

Una vez que se ha calculado la potencia de salida necesaria, ganancia y distancia que se necesita para transmitir la señal de RF y se ha seleccionado la antena apropiada para el trabajo, debemos motar la antena. Hay varias opciones para el montaje de una antena, ya sea esta en el interior o en el exterior.

Opciones para montaje de antena:

Montaje en el techo, típicamente colgada de algún herraje en la parte baja del techo.

Montaje en muro, por lo general se aplica a antenas direccionales, debido a que por un lado tiene el muro.

Montaje en columna, al igual que el muro pero en menor cantidad, es atenuada la señal por el extremo de la columna.

Montaje en poste, la antena se monta en la parte alta de un poste.

Montaje articulado, montaje en un poste con brazo movible.

Montaje en tri-pie, las antenas se montan en lo alto de un tri-pie.

Las antenas por lo regular deben ser escondidas, para evitar que cualquier persona pueda cuasar algún daño a estas. Algunos fabricantes hacen paneles para proteger las antenas. Se recomienda usar antenas para interior solo en interiores y antenas para exteriores, solo en exteriores; las antenas exteriores por lo general tienen mejor protección contra la humedad y los rayos de sol y plásticos que soportan altas temperaturas y bajas temperaturas, las antenas interiores no tiene estas características.

La orientación de una antena determina la polarización, y tiene un impacto significativo en la recepción de la señal. Si una antena es orientada con el campo eléctrico paralelo a la superficie de la tierra, entonces los clientes deberán también tener la misma orientación para una máxima recepción. Si el punto de acceso cambia su polarización también los clientes deben cambiar su polarización.

La alineación de una antena es algunas veces crítica y en otros no. Algunas antenas tienen u amplio el haz, ancho tanto por el lado horizontal como vertical. La alineación es muy importante cuando se quiere implantar enlaces de larga distancia usando antenas direccionales de alta ganancia. Cuando se usa antenas omnidireccionales o semi-direccionales, la apropiada alineación es cuestión de cubrir adecuadamente el área en que los usuarios inalámbricos puedan conectar sus dispositivos.

5.2.19 Dispositivos de energía sobre Ethernet (PoE)

Energía sobre Ethernet es una forma de entregar voltaje DC a un punto de acceso, puente inalámbrico (bridge), o cualquier otro dispositivo que soporte PoE, sobre un cable Ethernet Cat5, con el propósito de energizar al dispositivo. PoE es utilizado cuando no esta disponible una toma de corriente en el sitio donde se instala un dispositivo de red como un punto de acceso.

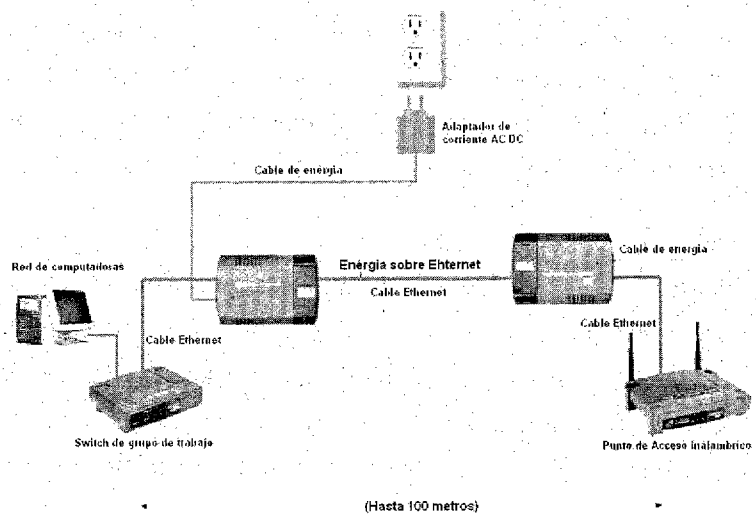


Figura 5.2.19-1 PoE

Es de gran ayuda ya que sobre esta forma so es necesario llevar un solo cable hacia el punto de acceso.

Aquí también la distancia máxima permitida es de 100 metros como se muestra en la Figura 5.2.19-1 es necesario saber antes de comprar si es necesario usar PoE, para poder seleccionar un punto de acceso que soporte PoE de lo contrario será un Punto de acceso con alimentación directa de una toma de AC.

Los dispositivos PoE están disponibles en algunos tipos como:

Inyectores de voltaje DC de puerto simple

Inyectores de voltaje DC de multi-puerto

Switch Ethernet diseñados para inyectar voltaje en cada uno de sus puertos.

PoE no es un estándar industrial, esto significa que cada fabricante tiene su versión adaptada a sus productos, difieren en voltajes y en la posición donde es

transportada la corriente DC, por lo que si se va usar PoE es necesario comprar los dispositivos de la misma marca para que estos sean compatibles con el punto de acceso que se va a utilizar. La IEEE esta trabajando en el estándar tales como 802.3af para PoE, pero todavía no hay un estándar definitivo

Hay dos tipos básicos de inyectores disponibles:

Inyectores pasivos

Inyectores protegidos

Cada tipo es típicamente disponible en una variedad de niveles de voltajes y numero de puertos.

Los inyectores pasivos ponen voltaje DC en un cable CAT5. Estos dispositivos no proporcionan protección contra corto circuito o sobre corriente.

Los inyectores protegidos proporcionan monitoreo y protección continua para detectar corto circuito y condiciones de sobre corriente en el cable CAT5.

5.2.20 Accesorios WLAN

Cuando sean necesario conectar todos los dispositivos WLAN juntos para formar una red, será necesario comprar los cables y accesorios apropiados para maximizar la entrega de datos dentro de la red LWAN, minimizar las perdidas de la señal y lo mas importante permitir la conexión adecuada de los dispositivos.

5.2.21 Amplificadores de RF

Los amplificadores de RF, amplifican o incrementan la amplitud de luna señal de RF. Este incremento de potencia es llamado ganancia y es medido en +dB. Un amplificador puede ser usado para compensar las perdidas presentes en la señal de RF, cualquiera que sea, como la distancia entre antenas, la longitud del cable entre el punto de acceso y la antena. La mayoría de los amplificadores son energizados

con corriente directa, pero a su vez estos inyectores de DC son alimentados de una toma de corriente alterna.

Los amplificadores vienen en dos tipos:

Unidireccionales

Bi-direccionales

Los amplificadores unidireccionales compensan las perdidas incurridas en la señal sobre los cables, a través de incrementar el nivel de la señal antes desea inyectada a la antena transmisora esto es son amplificadores de potencia de salida, o compensan las perdidas provenientes de la perdida en el espacio libre, esto es amplifican la señal de entrada a la antena. Los amplificadores de este tipo por lo regular se instalan antes de la antena ya sea en el exterior o en el interior. Los amplificadores bi-direccionales .hacen las dos funciones lo cual implica que se puede instalar en el mismo cable, después de un duplexor si es que existe este. Mientras que los unidireccionales se instalan por lo regular antes del duplexor donde la señal de entrada (Rx) y la señal de salida (Tx) están separadas.

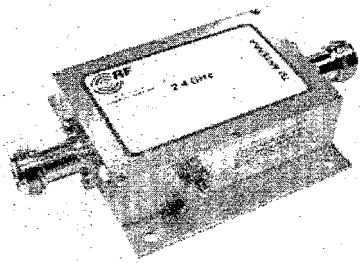


Figura 5.2.21-1 Amplificador WLAN

La mayoría de los dispositivos WLAN utiliza amplificadores bi-direccionales, esto es amplifican la señal de entrada y de salida. Para la seleccione de un amplificador se debe tomar en cuenta: la impedancia, la ganancia, la respuesta a la frecuencia, VSWR, potencias de entrada y salida del amplificador.

Los amplificadores usados para WLAN son instalados en serie con la trayectoria de la señal principal.

5.2.22 Atenuadores de RF

Un atenuador de RF, es un dispositivo que causa precisamente una perdida de la señal de RF medida. (En dB), esto es, disminuye el nivel de la señal de RF, contrario a lo que hace un amplificador. Los atenuadores permiten reducir en nivel de la señal de RF de salida, cuando el arreglo ganancias de antena y punto de acceso, exceden los niveles permitido, un atenuador con la atenuación adecuada permite tener una potencia de salida que este dentro de lo permitido. También nos sirve para controlar el área de cobertura de un punto de acceso, limitando el nivel de la señal de RF, para evitar que la señal llegue a distancia a las cuales no es necesario.

Hay atenuadores fijos y variables. Los atenuadores fijos vienen en diferentes valores

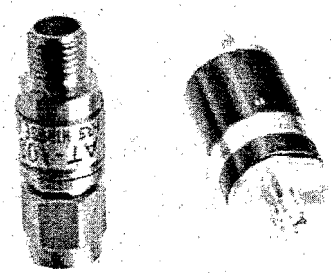


Figura 5.2.22-1 Atenuadores SMA

de atenuación y con diferentes tipos de conexiones. Los atenuadores variables son atenuadores que se pueden variar, pudiendo aplicar la cantidad de atenuación necesaria con un solo atenuador. Tipicamente son utilizados para el estudio de

campo para determinar la ganancia de antena, niveles de amplificación, etc. Los atenuadores son instalados en serie con la línea de transmisión, por un extremo entra la señal proveniente del punto de acceso y por el otro sale con dirección hacia la antena.

5.2.23 Supresores de transitorios

Los supresores de transitorios ("Arrestors") son usados para enviar a tierra señales transitorias de alta corriente, provocadas por las descargas eléctricas naturales. Los supresores de transitorios son utilizados para proteger el hardware WLAN, tales como puntos de acceso, bridges, y una tarjeta de red inalámbrica acoplada a una antena externa.

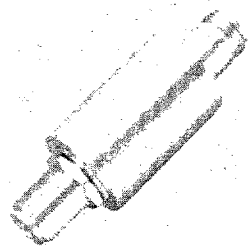


Figura 5.2.23-1 Supresor de transitorios

Los supresores de transitorios son instalados en serie con la línea de RF (coaxial), y son conectados a tierra para permitir enviar los transitorios hacia tierra y no al equipo. Están diseñados para permitir el paso de la señal de RF pero no los transitorios provocados por descargas eléctricas. La mayoría de los supresores de transitorios son capaces de disparar un corto hacia tierra en menos de 2 microsegundos, pero las especificaciones de la IEEE, dicen que el proceso no debería de pasar en más de 8 microsegundos. Es muy importante que no se rebase el valor fijado por la IEEE.

Para la selección del supresor de transitorios se recomienda revisar al menos los siguientes parámetros para que sea compatible con equipos WLAN:

Tipo de conectores

Impedancia

Perdida por inserción

Frecuencia de operación

Potencia de operación

5.2.24 Divisores de RF

Un divisor es un dispositivo que tiene un conector de entrada único y múltiples conectores de salida. El más común es una entrada por dos conectores de salida. Los divisores son usados con el propósito de dividir una señal en múltiples señales de RF independientes. Una situación en la cual se podría usar un divisor seria cuando se quiere radiar en dos direcciones opuestas y para hacer esto se requiere un divisor con dos antenas direccionales, cada una de las antenas seria conectada a cada una de las salidas del divisor, también debe considerarse la pérdida por inserción del divisor.

Para la selección del un divisor se debe tener en cuenta los distintos parámetros de operación de los dispositivos WLAN.

Figura 5.2.24-1 Divisor de RF

Debe procurarse no utilizar estos dispositivos por que además de resultar caros incrementar la perdida por inserción y requiere el uso de mas de un antena por sitio de repetición.

5.2.25 Conectores de RF

Los conectores de RF son aquellos utilizados en las líneas de transmisión coaxial o guías de ondas. Para seleccionar el tipo de conector ha ser utilizado se debe tener en cuenta varias consideraciones, las cuales listamos a continuación:

1. los conectores debe ser de la misma impedancia de los dispositivos WLAN (por lo común 50 ohms).
2. las pérdidas por inserción de cada conector insertada en la ruta de la señal, deben ser consideradas en el cálculo dado que si son de consideración. Se debe seleccionar los conectores con menor perdida por inserción.
3. el rango de frecuencia de operación de los conectores, esto debido a que las WLAN pueden ser de 2.4 GHz o de 5 GHz. Algunos conectores trabajas dentro de ciertos rangos de frecuencia por lo que es importante saber en que banda de frecuencia trabajan y si son los apropiados para WLAN.

4. la calidad de los conectores debe ser la adecuada, existen diferentes marcas de conectores pero no todos tienen la misma calidad, esto puede afectar el rendimiento de nuestra red, se recomienda comprar conectores de marcas conocidas y de la mejor calidad de este fabricante, esto puede ayudar a eliminar muchos problemas de asociados con señales de RF esporádicas, VSWR y malas conexiones.

5. se debe conocer de antemano el tipo de conector a ser utilizado (N, F, SMA, etc.) y el sexo del conector, ya sean estos hembras o machos. Los conectores machos vienen con un pin central, mientras que los conectores hembras vienen con una conexión central donde entra el pin del otro tipo de conector, siendo estos complementarios.

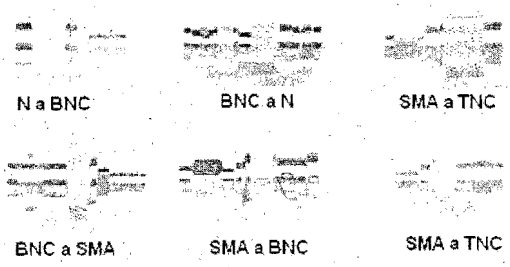


Figura 5.2.25-1 Conectores de RF

5.3 Medios de transmisión.

Los medios de transmisión son la parte pasiva a través del cual se puede enviar una señal en banda base o banda ancha, eléctrica, electromagnética u óptica que contenga información y que se desee enviarse de un punto a otro, este es uno de los puntos mas críticos ya que este define en gran medida el ancho de banda para un sistema de comunicación.

5.3.1 Par trenzado

La aplicación mas común del par trenzado es en el sistema telefónico, se puede tener varios kilómetros de par trenzado sin necesidad de amplificación, pero se necesitan repetidores para distancias mayores, los pares de estos haces interferirían unos con otros si no fuera por el entrelazamiento.

Figura 5.3.1-1Cable UTP

Los pares trenzados se pueden usar tanto para transmisión analógica como digital. El ancho de banda depende del grosor del cable y de la distancia, pero en muchos casos se pueden lograr varios mega bits/seg. Durante algunos kilómetros. Los pares trenzados se usan ampliamente debido a su rendimiento adecuado y a su bajo costo.

El cableado de par trenzado tiene algunas variaciones, dos de las cuales son importantes para las redes de computadoras. Los pares entrelazados de la categoría 3 consisten en dos hilos aislados que se entrelazan de manera delicada. Cuatro de estos pares se agrupan por lo regular en una funda de plástico para su protección y para mantener juntos los ocho hilos.

Los pares trenzados de categoría 5 son similares a los de categoría 3, pero con más vueltas por centímetro y con aislamiento de teflón, lo cual produce menor diafonía y una señal de mejor calidad a distancias mas largas, lo que los hace mas adecuados para la comunicación de computadoras a altas velocidades. Ambos tipos de cableado recibe el nombre de UTP (unshielded twisted pair, par trenzado sin blindaje).

5.3.2 Características.

La TIA/EIA, dos grupos que establecen los estándares para datos industriales adopto el plan de separar las velocidades de envío de datos y otros parámetros, en categorías, debido a esto ahora tenemos las categorías 3 y 5. Cada categoría en forma ascendente presenta mayores rendimientos que la categoría previa.

Impedancia. Indica la Habilidad del cable para fijar y transferir la energía de un extremo a otro. La impedancia del cable es determinada por la impedancia de los sistemas. La TIA/EIA estandariza para la categoría 5, 100 ohms ± 15 ohms.

Ancho de banda. Es el rango de frecuencia disponible para ser usada por la señal portadora. El ancho de banda solo es usado para comparar la capacidad de manejo de datos y no es función del tipo de compresión que se quiera utilizar para el envío de datos y es expresado en Mhz.

Atenuación. Es la perdida de señal y es característica de todos los sistemas.

N.E.X.T Indica como un par activo puede afectar en forma adversa, la calidad de transmisión de otro par en el cable. Frecuentemente expresado en dB de aislamiento, a valores mayores de este mejor integridad de la señal.

Nivel 6 y 7.

Un distribuidor, Anixter ha instituido un programa para determinar los niveles 6 y 7, es su propio estándar y no tiene que ver con alguna organización de estándares.

5.3.3 Cable coaxial de banda base.

Este cable tiene mejor blindaje que el par trenzado, así que puede abarcar tramos más largos a velocidades mayores. Son dos las clases de cable coaxial mas utilizados. El cable de 50 ohms, se usa comúnmente para transmisión digital, la otra

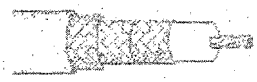


Figura 5.3.3-1 cable coaxial banda base

clase es el cable de 75 ohms, se usa comúnmente para la transmisión analógica.

Un cable coaxial consiste en un alambre de cobre rígido como núcleo, rodeado por un material aislante y este a su vez, esta forrado por una malla tejida de material conductor, por ultimo este se forra con un material aislante.

La construcción y el blindaje del cable coaxial le confieren una buena combinación de elevado ancho de banda y excelente inmunidad al ruido. El ancho de banda posible depende de la longitud de este. En cables de 1 km. es factible una velocidad de datos de 1 a 2 Gbps. También se pueden usar cables más largos, pero a velocidades de datos más bajas o con amplificadores periódicos.

5.3.4 Coaxial RGB.

Es utilizado para enviar en forma separada señales de rojo verde y azul (Red, Green y Blue) en aplicaciones de vídeo. Este tipo de cable viene en 3, 4 o 5 conductores con código de color para fácil identificación, el cable depende de los componentes de la transmisión, para RGB cable con 3 conductores, para RGB y Sync un cable de 4 conductores, para RGB, Sync y Hold un cable de 5 conductores.

5.3.5 Coaxial SVHS.

El formato súper VHS (SVHS) requiere dos conductores separados para transmitir la luminancia y crominancia. La crominancia contiene información del color y la luminancia indica la cantidad de iluminación.

5.3.6 Coaxial compuesto.

Cable coaxial compuesto para aplicaciones de cámara donde se requiere uno o más cables coaxiales para vídeo y uno o más cables pares blindados para audio y energía.

5.3.7 Cable coaxial de banda ancha

Aunque el termino banda ancha viene del mundo de la telefonía, donde se refiere a cualquier cosa mas ancha que 4 KHz, en el mundo de las redes de computadoras "cables de banda ancha significa cualquier red de cable que utilice transmisión analógica.

Figura 5.3.7-1 Cable coaxial de banda ancha

Puesto que las redes de banda ancha emplean tecnología estándar de la televisión por cable, los cables se pueden usar hasta 300 MHz (y con frecuencia hasta 450 MHz) y pueden extenderse distancias de hasta 100 km. gracias a la señalización analógica, que es mucho menos critica que la digital.

Los sistemas de banda ancha se dividen en múltiples canales, con frecuencia los canales de 6 MHz que se usan para la difusión de la televisión.

Los sistemas de cable dual tienen dos cables idénticos que corren en paralelo, uno junto al otro. Para transmitir datos, la computadora envía los datos por el cable 1, que conduce a un dispositivo llamado head-end en la raíz del árbol de cables. A continuación, el head-end transfiere la señal al cable 2 para transmitirla de regreso por el árbol. Todas las computadoras transmiten por el cable 1 y reciben por el cable 2.

5.3.8 Líneas de transmisión.

Una línea de transmisión consta de dos o más conductores paralelos que se usan para conectar una fuente a una carga o un circuito a otro. Una línea de dos conductores, en general de configuración coaxial puede transportar megawatts de potencia desde un transmisor a una antena o usarse para transportar picowatts de potencia de la señal recibida desde una antena a un receptor.

Las líneas de transmisión requieren por lo menos dos conductores para el modo EMT (electromagnético transversal). El rango de operación va de 30 MHz hasta cerca de 30 GHz

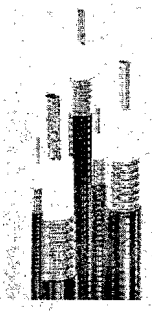


Figura 5.3.8-1 Líneas de transmisión

5.3.9 Fibra óptica

Los cables de fibra óptica son similares a los coaxiales, excepto por el trenzado. El núcleo esta en el centro, y a través de el se propaga la luz. En las fibras multi-modales el diámetro es de 50 micras, en las fibras mono-modo el núcleo es de 8 a 10 micras. El núcleo esta rodeado por un revestimiento de vidrio con un índice de refracción menor que el del núcleo, a fin de mantener toda la luz en el núcleo. A continuación viene una cubierta plástica delgada para proteger al revestimiento. Las fibras normalmente se agrupan en haces, protegidos por una funda exterior.

Las fibras pueden conectarse en tres formas diferentes. Primera, pueden terminar en conectores e insertarse en enchufes de fibra. Los conectores pierden casi el 10 o 20 % de la luz, pero facilitan re-configuraciones de los sistemas.

Segunda, se pueden empalmar de manera mecánica, los empalmes mecánicos acomodan dos extremos cortados con cuidado uno junto a otro en una manga especial y los sujetan en su lugar. Se puede mejorar la alineación haciendo pasar luz por la unión y efectuando pequeños ajustes para maximizar la señal. Los empalmes mecánicos toman al personal entrenado cerca de 5 minutos y resultan en una perdida de luz de 10 %.

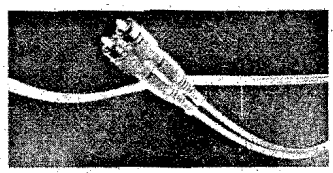


Figura 5.3.9-1 Fibra óptica

Tercera, se pueden fusionar (fundir) dos extremos de fibra para formar una conexión sólida. Un empalme por fusión es casi tan bueno como una fibra de hilado único, pero aun aquí hay un poco de atenuación. Con los tres tipos de empalme pueden

ocurrir reflejos en el punto del empalme y la energía reflejada puede interferir la señal.

Se pueden utilizar dos clases de fuente de luz para producir las señales, LED (diodos emisores de luz) y láseres semiconductores.

EL extremo receptor de una fibra óptica consiste en un fotodiodo que emite un pulso eléctrico cuando lo golpea la luz.

5.3.10 Espacio libre.

Es utilizado para las comunicaciones inalámbricas ya sea para comunicación de alta capacidad o canales de baja capacidad (voz y datos), cuando la señal electromagnética viaja a través de el sufre efectos que inducen ruido en la señal original entre los cuales se encuentran:

5.3.11 Desvanecimiento por absorción

Es la atenuación de la onda se radio causada por absorción o dispersión debido a la lluvia, nieve, neblina, gas molecular en la ruta de propagación. Tiene mayores efectos en rangos por encima de los 10 GHz.

5.3.12 Atenuación debido a obstáculos.

La señal recibida sufre decremento por interrupción del rayo electromagnético debido a obstáculos causados por variaciones en el índice de refracción.

5.3.13 Atenuación por interferencia.

El desvanecimiento por interferencia, también llamado desvanecimiento por multi-trayectoria ocurre cuando: dos o mas rayos con diferente longitud debido a reflexión o refracción es recibida en el punto receptor.

Capitulo 6 Seguridad en las redes WLAN 802.11

6.1 Principios de seguridad

La palabra seguridad puede significar muchas cosas dependiendo del contexto al que se refiera por ejemplo podemos hablar de seguridad en relación a la policía municipal o federal, seguridad personal, riesgos financieros y privacidad en las comunicaciones. También podemos referirnos a seguridad a un estado de emoción personal.

Se puede definir seguridad en términos de dos grupos, "los chicos buenos" y "los chicos malos", sin importar de quien se este hablando, de personal, de computadoras, o robots, si no hay chicos malos, entonces por default estamos seguros, pero la vida no es perfecta y si los hay. El no pensar en seguridad solo significaría que no trae graves consecuencias vivir en un entorno inseguro.

Las buenas medidas de seguridad empiezan mucho antes de implementar un sistema cualquiera que sea este, incluso una red inalámbrica. A continuación listamos estos principios:

1. No hablar con nadie sobre lo que se piensa hacer.
2. No aceptar a nadie sin una garantías
3. Trata a cualquier como a un enemigo hasta que este pruebe lo contrario
4. No trates a tus dispositivos de comunicación por largo tiempo
5. Usa soluciones bien probadas
6. Observa el lugar donde estas y revisa las fallas.

6.1.1 No hablar con nadie sobre lo que se piensa hacer.

En el contexto de seguridad esto significa que debemos estar seguros al 100 % sobre la identidad de un dispositivo o persona antes de comunicarnos en estos. Para un LAN inalámbrica no es suficiente verificar la identidad de la otra parte. Las LAN inalámbricas deben también verificar todos los mensajes que vienen desde la otra parte (un cliente inalámbrico cualquiera). Un método simple de autenticar a alguien

es requerirle que conozca una clave secreta, esto debe ser establecido al inicio de la comunicación para establecer su identidad y entonces la clave secreta puede ser incorporada en cada mensaje para asegurar la autenticidad de cada mensaje, la idea es que cualquier enemigo no pueda sustituir sus mensajes malos por un mensaje autentico, esto debido a que el enemigo no conoce la clave secreta que debe incorporarse en cada mensaje. Esta idea fue el principio básico del protocolo de seguridad llamado WEP.

6.1.2 No aceptar a nadie sin una garantía

Como seguridad, la palabra garantía significa diferentes cosas para diferentes personas. En el contexto de seguridad en redes inalámbricas significa garantía de autenticidad, en otras palabras, se debe probar que el mensaje no ha sido cambiado. La persona o el equipo deben probar su identidad antes que aceptemos sus mensajes, pero también nosotros necesitamos estar seguros que estamos recibiendo un mensaje que es enviado por una persona o equipo valido y que el mensaje no ha sido modificado, retardado o remplazado con un nuevo mensaje de un enemigo.

6.1.3 Trata a cualquier como a un enemigo hasta que este pruebe lo contrario

En una red LAN alambrada, por ejemplo tenemos una idea bastante buena de donde estamos conectados debido a que normalmente nos conectamos en una red empresarial o una red casera, y ambas son un red aislada y encerrada donde solo se conectan personas que en teoría están bien identificados (por que son miembros de la misma organización), están autorizados para conectarse y comparten un fin común, el trabajo en equipo por que nos sentimos seguros. Mas sin embargo por diseño los clientes WLAN pueden monitorear las señales de RF de un punto de acceso y tratar de asociarse a una red en particular. Los puntos de acceso advierte su presencia a través de la transmisión de los beacons (frames de señales guía) con su identidad, por lo que un enemigo cualquiera puede tratar de asociarse y falsificar

mensajes que demuestren que el es parte de la red. Parte de al seguridad es evitar que un enemigo trate de pasarse como un cliente valido.

6.1.4 No trates a tus dispositivos de comunicación por largo tiempo

Los buenos chicos pueden ser identificados en una red inalámbrica debido a que ellos poseen una señal (la clave secreta) que puede ser verificada. Tales señales como claves, certificados o llaves. Necesitan tener un tiempo de vida limitado. De esta manera podemos reafirmar la relación a través de la renovación de la clave. Fallas en este paso pueden resultar en sorpresas inesperadas.

Hay diferencias entre políticas y protocolos. En términos simples los protocolos de seguridad están diseñados para implementar las políticas de seguridad. Las políticas de seguridad como decidir quien es de confianza, a donde se pueden conectar y donde no, cuando esta permitido conectarse, etc., son tomadas por personas como un administrador de red y es entonces el trabajo de los protocolos de seguridad en conjunción con el software y hardware evitar que cualquier cliente o dispositivo rompa las políticas de seguridad

Los equipos como tarjetas de red inalámbricas o incluso computadoras portátiles, pueden ser robadas y utilizadas para accesar a la red inalámbrica, este es un de los motivos por los que se debe cambiar constantemente las clave.

6.1.5 Usa soluciones bien probadas

Actualmente existen diferentes protocolos de seguridad que trabaja de forma distinta y en algunos de los casos pueden ser utilizados mezclando dos o más. Se recomienda sin embargo, utilizar los protocolos y medidas de seguridad bien probados por organismos especializados y estar al pendiente de los nuevos protocolos de seguridad, también es conveniente investigar si algún protocolo de seguridad ya a sido roto. Existen aplicaciones de seguridad que no se guían por estándares o que son una variación de un estándar y son comercializados por empresas argumentando que son superiores en cuanto a seguridad en relación a un

estándar fijado por un organismo internacional, para que un protocolo o medida de seguridad se considere segura deben pasar por diferentes parte, organismos internacionales, especialistas en seguridad, revistas especializadas en pruebas de hardware y software e incluso un numero considerable de usuarios, realizando pruebas durante un periodo de tiempo considerable, entonces podemos estar seguros que es un protocolo o medida de seguridad confiable, como ejemplo considere el protocolo de seguridad WEP que fue el primer protocolo de seguridad implementado en las redes WLAN y que a la fecha ya a sido rota y descifrado por lo que este protocolo no es la mejor opción para mantener segura una red inalámbrica.

6.1.6 Observa el lugar donde estas y revisa las fallas.

Cuando se considera implantar una red inalámbrica se debe ver no solo el lugar físico sino también el entorno donde se va a implementar esta. Por ejemplo una red inalámbrica no solo requiere medidas de seguridad en la transmisión de los paquetes inalámbricos sino también se requiere poner el equipo en un lugar que sea razonablemente seguro y donde ninguna persona ajena a la red inalámbrica tenga acceso, la ubicación de los elementos de la red no deben ser divulgados para evitar que cualquier persona mal intencionada

6.2 Ataques a las redes WLAN

Los ataques a las rede inalámbricas pueden ser clasificados en cuatro categorías: husmear, modificación, disfrazarse, y negación del servicio.

6.2.1 Husmear (snooping)

Como su nombre sugiere, en este modo un hacker solo esta simplemente accesando a información privada. Esta información puede usarse como una ventaja, tales como obtener secretos de la compañía que ayuden a alguien a hacer un negocio, decisiones de compra. Y pueden ser usados para realizar actos delictivos en un momento menos preciso para la empresa, como el día de pago del aguinaldo, las fechas de pago a proveedores, etc.

6.2.2 Modificación

La modificación de información por parte de un hacker puede dañar gravemente nuestra situación económica o social, por ejemplo si un hacer modifica un mail que es enviado a nuestro jefe, y el hacer modifica la información de tal manera que cuando nuestro jefe lo lea, y compruebe los resultados físicos de nuestro reporte pensara que somos unos mentirosos y que le enviamos información falsa para que este quede mal con sus superiores. Otra situación podría ser cuando enviamos un mail a un banco sobre un posible retiro, un hacker podría modificar las cifras del retiro y de la posible cuenta a donde deseemos depositar el retiro.

6.2.3 Disfrazarse

Los hacker podrían tomar estrategias que le permitan demostrar a la red (punto de acceso y servidores de acceso) demostrar que el es un usuario valido y de esta manera poder utilizar los recurso de la red como el uso de Internet. Cuando un administrador este escaneando la red simplemente no vera al hacker debido a que este ha tomado la identidad de otro usuario.

6.2.4 Negación de servicio

Cuando un hacker realiza un ataque de negación de servicio (DoS) bloquea todo el tráfico de la red. El objeto de ataque de DoS es causar daño a la red a través de impedir la operación de la red incluso para el hacker.

6.3 Seguridad en redes Wi-Fi

Cuando nos comunicamos por Internet usando una conexión por cable o inalámbrica, podemos querer asegurar la comunicación protegiendo los datos privados y los archivos. Si nuestras transmisiones no son seguras, tomaremos los riesgos de que otros intercepten nuestros emails, examinen nuestros archivos corporativos y usen nuestra red y la conexión de Internet para distribuir sus propios mensajes.

Como asegurar nuestra red puede sé dependiente de como usamos la red. Si estamos navegando para investigar o ver películas, podemos no preocuparnos si cualquier recoge parte de la transmisión. Si estamos comprando artículos sobre la red, estas transacciones financieras son usualmente protegidas por una tecnología llamada capa de conexión segura (SSL, Secure Socket Layer) Sin embargo si nuestros datos son confidenciales o si queremos seguridad adicional, hay algunas tecnologías diferentes que podemos considerar para ser implementadas.

En una red inalámbrica casera, podemos usar una variedad de procedimientos de seguridad simples para proteger la conexión Wi-Fi. Estas incluyen encriptación habilitada de 64 y 128 bits (WEP, privacidad equivalente en cable), cambiando nuestro password y nombre de red y encerrando nuestra red. Estas técnicas básicas trabajan en ambas, oficinas pequeñas y compañías grandes. Sin embargo podemos usar también emplear adicionalmente más tecnologías sofistificadas y técnicas para promover la seguridad de la red.

Hay muchas opciones disponibles para ayudar a asegurar las WLAN. Es son:

WEP	Filtros de MAC	Antenas de radiación por zona
DMZ	Firewalls	VPNs
RADIUS	TKIP	AES
SSL	IDSs	

La seguridad de los distintos estos distintos medios esta basada en parte en procedimientos de encriptación. La encriptación es una algoritmo que permite modificar el modificar la información de manera que no se entendible por otra persona que no sea el destinatario original. Para entender la seguridad en redes inalámbricas es preciso describir algunos conceptos básicos de encriptación.

6.3.1 Algoritmo

Algoritmo es un conjunto explícito de instrucciones que tienen un punto de inicio y fin definido. Por ejemplo. Las instrucciones que nosotros seguiríamos para configurar una VCR son consideradas un algoritmo. En realidad, nosotros desarrollamos algoritmos paso por paso todo el tiempo. Cualquier cosa desde arrancar un carro hasta cocinar un pan puede ser definido como un algoritmo.

6.3.2 Criptografía

Criptografía es el estudio de los algoritmos de encriptación y des-encriptación. Encriptar es similar a revolver los datos o mensajes a través de un algoritmo, lo opuesto es des-encriptar. La encriptación es típicamente acompañada con la asistencia de un parte de datos externos, los cuales frecuentemente vienen en la forma de un password de un usuario seleccionado. Esto no solo hace la encriptación robusta a través de forzar una clave única, pero también mantiene fuera a los usuarios que no conocen el password para acceder a los datos.

Hay dos tipos principales de encriptación: simétrica y asimétrica cada uno tiene su fortaleza y debilidad y son convenientemente mejores para una específica aplicación.

6.3.3 Encriptación simétrica

Los procesos de encriptación y des-encriptación simétricos son realizados usando la misma clave. Esta es la más prevaleciente forma de encriptar. Supongamos que queremos encriptar la palabra "Wireless" usando como clave el password "wep", la operación seria así:

Tomamos la palabra Wireless y cambiemos cada letra con su correspondiente valor alfanumérico.

Cambiemos cada letra de password "wep" y cambiemos las letras por su correspondiente valor alfanumérico.

Sumamos las cifras que representan a las palabras "Wireless" y "wep", en el caso de la palabra "wep", hacemos una cadena de izquierda a derecha con la misma, hasta tener el mismo número de cifras que tiene la palabra "Wireless".

Ahora el resultado es nuestro texto cifrado.

Ahora tenemos un proceso de encriptación de una palabra cualquiera, para des-encriptar el texto cifrado, simplemente aplicamos el proceso en forma inversa, obviamente debemos conocer el password que esta funcionando como clave en el proceso de encriptación.

La encriptación simétrica es mucho más rápida que la encriptación asimétrica, sin embargo la dificultad con la encriptación simétrica, es que la seguridad depende de mantener el password secreto.

6.3.4 Encriptación asimétrica

Esta encriptación es mucho más compleja, pero tiene el potencial de ser más segura. Un numero grande de aplicación esta incorporando este tipo de seguridad. Aplicaciones de email, VPNs, PKI e incluso proveedores de servicios de aplicaciones usan encriptación asimétrica.

La encriptación asimétrica requiere del uso dos claves, una publica una privada. Cada clave requiere del uso de la otra para descifrar un mensaje, como ejemplo, supongamos que mi jefa quiere enviarme un mensaje seguro y para que este se mantenga confidente, que solo yo pueda abrirlo. Ella puede encerrar el mensaje en una caja usando un candado para el cual solo yo tengo la llave. Así ninguno incluso mi jefa podrá abrir el mensaje sin el uso de mi llave (clave privada) En este caso la cerradura seria la llave publica.

6.3.5 Desventajas y ventajas de la encriptación

Hay múltiples beneficios de la encriptación. Por ejemplo puede ser usada para autenticar usuarios autorizar acceso a recursos, asegurar la confidencialidad de datos y garantizar la integridad de los datos.

Sin embargo hay también algunos inconvenientes potenciales con la encriptación, estos inconvenientes son la perdida de password, falsas percepciones de seguridad y el procesamiento excesivo de overhead (encabezados en los datos) usando encriptación.

6.3.6 Pérdida de password

Un problema con la encriptación es, que hacer en el caso de la perdida del password. En este caso la única opción es buscar un método para romper el password. Sin embargo dependiendo del método de encriptación, pueden pasar algunos años antes de que podamos extraer datos, en adición a esto en algunos países, incluyendo los estados unidos, consideran de cualquier acto de romper un password es ilegal, incluso si los datos son los propios.

6.3.7 Falsas percepciones de seguridad

Muchas personas consideran sus redes están seguras solo por el hecho de usar WEP. Esta suposición es falsa. En algunos casos el password es puesto en blanco en otros ponen en password por default. En adición WEP no protege contra la mayoria de los ataques de hackers, finalmente WEP es fundamentalmente débil. Se recomienda usar WEP pero no como su única línea de defensa.

Los password son buenos solo si no son compartidos o pueden ser obtenidos de cualquier medio o son fáciles de adivinar.

6.3.8 Sobre encabezado debido a la encriptación

El tiempo de utilización de CPU que es tomado para encriptar y des-encriptar datos de red. Este overhead puede tener un serio impacto en la productividad de las aplicaciones de red y puede tener resultados perjudiciales en situaciones de tiempo crítico. Cualquier encriptación adiciona overhead (encabezados de control) para los requerimientos de procesamiento de un sistema en red, retrasa los procesos de transmisión y puede también afectar adversamente a las habilidades de los dispositivos procesadores de la red.

6.4 Cifrado

Hay dos métodos principales por los cuales los datos pueden ser encriptados

6.4.1 Cifrado de bloque

Un bloque cifrado (tales como DES o 3 DES) toma una cadena larga de datos lanzados y los encripta con la clave. Este proceso es repetido una y otra vez hasta que el mensaje intacto completamente encriptado. Típicamente hay una variable de tamaño que controla que tan grandes los datos enviados pueden ser. Sin importar el tamaño de los bloques el mensaje es enviado completo.

Por ejemplo supongamos que yo quiero enviar un email a mi jefa usando cifrado por bloque, en este caso en este caso yo necesito un password y en mensaje entero deberá ser encriptado de una vez.

Hay que observar que cuando dos bloques de datos son encriptados con la misma clave, la clave puede ser extraída del texto cifrado. En otras palabras, si un atacante puede determinar los datos originales de un mensaje, él puede comparar el texto cifrado con el texto plano y calcular la diferencia. Esta diferencia será entonces el código para crackear cualquier futuro mensaje encriptado.

6.4.2 Cifrado de flujo

El cifrado de flujo también usa una palabra como password, sin embargo, encripta datos en una escala mucho más pequeña. Mientras que la encriptación por bloque puede encriptar una página de texto de una sola vez, el cifrado de flujo, puede encriptar los bits que hacen a las letras de la página de texto. Supongamos que la letra "A" es convertida a código ANSI con un valor de 65, este a su vez es convertida en un Byte que comprende 8 bits. El cifrado de flujo puede encriptar un bit antes de que sea enviado a la salida y se repite el proceso de encriptación siete veces mas para una letra. Esto puede resultar en miles de valores encriptados para en texto cualquier.

El cifrado de flujo es capaz de encriptar en un nivel detallado, debido a que usa una condición de estado además de los datos y el password. Esto significa que los datos son encriptados de forma diferente para cada envió que pasa a través del programa de encriptación. Para hacer un cifrado de flujo, son generados dos flujos, uno para alimentar a le otro. El primer flujo es llamado "el flujo clave", el cual combina un valor de estado, valores de datos y el password, para generar un flujo de datos aleatorios. El flujo clave en turno es usado para producir una salida cifrada combinando un nuevo valor de estado (desde el flujo clave), valores de datos y valores clave.

6.4.3 Auto sincronización de cifrado de flujo

Las siguientes son dos funciones de auto sincronización de cifrado de flujo:

$State_{Time+1}$ = State Funtion ($State_{Time}$, $Data_{Time}$, $Password_{Time}$)

$Output_{Time}$ = Cipher Function($state_{Time}$, $Data_{Time}$, $Password_{Time}$)

Como se ilustra, la salida es ahora dependiente de tres variables, dos de las cuales serán cambiantes (el password es constante) La primer función es conocida como el generador de flujo clave y la segunda es la función de cifrado.

La fortaleza de este tipo de encriptación es encontrada en el hecho de que ahora hay dos variables que cambian. Por lo tanto, incluso si hay un valor predecible en los datos, el estado será aleatorio, diferente, lo cual significativamente decrece las oportunidades de un ataque.

Hay dos variaciones del cifrado de flujo, estas son conocidas como cifrado de flujo sincrono y cifrado de flujo auto sincronizado. La diferente entre las dos es encontrado en si la clave de flujo confía en los datos para producir el flujo. El ejemplo anterior ilustra como un cifrado de flujo auto sincronizado, como confía en los datos para producir una clave de flujo. En contraste, el siguiente ejemplo ilustra como un cifrado de flujo asíncrono crea la salida. En este tipo de cifrado, las primeras dos funciones combinadas son consideradas por el generador de clave de flujo.

$State_{Time+1}$ = State Funtion ($State_{Time}$, $Password_{Time}$)

Stream $Value_{Time}$ = Keystream Funtion($State_{Time}$, $Password_{Time}$)

$Output_{Time}$ = Cipher Funtion (Stream $Value_{Time}$, $Data_{Time}$)

Aunque el cifrado sincrono parece mas complicado, es actualmente débil como lo es el cifrado auto sincronizado notemos en la ultima función que para obtener algún dato solo requerimos un valor desconocido para invertir el proceso de cifrado. Por el otro lado, el cifrado de flujo auto sincronizado, usa tres variables.

6.5 Tecnologías de seguridad 802.1x y otras.

Con el crecimiento exitoso y adopción de las redes Wi-Fi, muchas otras tecnologías de seguridad han sido desarrolladas y continúan siendo desarrolladas. La seguridad es una constante desafió, y hay cientos de compañías desarrollando soluciones desde cualquier punto de vista.

Hay una variedad de soluciones de seguridad propias de terceras partes que efectivamente pasan por alto el estándar de transmisión Wi-Fi y proporcionan

encriptación, Firewall y servicios de autenticación. Muchos fabricantes de dispositivos Wi-Fi también han desarrollado tecnologías de encriptación propietaria, que aumentan grandemente la seguridad básica de Wi-Fi.

Técnicas de encriptación usan tecnologías especiales para encriptar la información en un extremo y del otro extremo des encriptar la información. Otras técnicas usan claves especiales o códigos que permiten a las computadoras comunicarse entre sí, la computadora que envía transmite una clave o código para ser recibida por la computadora receptora, y si la clave es igual, la computadora que envió se le permite ingresar al sistema.

La alianza Wi-Fi, el comité del estándar 802.11 y muchos miembros de Wi-Fi están trabajando para desarrollar nuevos estándares de seguridad tales como 802.11i y 802.1x. Estos nuevos estándares de seguridad usaran avanzadas tecnologías de encriptación tales como AES y TKIP, tan bien como son seguros los métodos de distribución de claves.

Los hackers pueden romper los códigos de encriptación interceptando y analizando grandes cantidades de datos, pero romper códigos toma tiempo. Pero cambiando automáticamente las claves de encriptación cada 5 minutos (por ejemplo), las redes Wi-Fi están ya usando un nuevo código para el tiempo en que el hacker ha interceptado y roto los códigos del anterior.

La mayoría de las redes Wi-Fi de nivel empresarial ya permiten a los administradores de IT cambiar el código manualmente, pero el estándar 802.1x hace el proceso automático.

6.6 Establecimiento de tecnologías juntas

Individuos y compañías que tiene el deseo de ir más allá de los mecanismos de seguridad básica pueden elegir implementar y combinar estas tecnologías básicas para incrementar la protección de sus trabajadores móviles y sus datos. Como con

cualquier red, por alambre o inalámbrica, a medida que se incrementan mas capas de seguridad, la transmisión de datos puede ser más segura.

6.7 Seguridad en espacios públicos

Las redes inalámbricas en áreas públicas y HotSpots como cafés Internet no pueden proporcionar cualquier seguridad. Aunque algunos proveedores de servicio proporcionan esta (seguridad) con el software del cliente, muchos HotSpots permiten toda su seguridad apagada para hacer fácil el acceso a la red en el primer intento.

Si no se dispone de medidas de seguridad se recomienda usar las redes inalámbricas solo para áreas no críticas, como navegar por Internet.

Las buenas noticias son que muchos proveedores de HotSpots y fabricantes de Wi-Fi están implementando mejores tecnologías de seguridad para proteger a los usuarios de Wi-Fi contra interceptaciones y monitoreo de las transmisiones en HotSpots públicos.

6.8 WEP

Aunque este tiene una palpable debilidad y es cierto que la versión WEP actual se puede romper. Sin embargo la mayoría de las personas que intentan accesar una red inalámbrica, no pondrán empeño en tratar de romper la encriptación WEP. Los Hacker curiosos verán que la red usa WEP y mejor se irán hacia una red abierta sin protección. Esto por que no tienen la paciencia y actitud para penetrar la protección exitosamente. En otras palabras, utilizando la protección WEP, podemos eliminar hasta el 99 % de los intentos. Esto solo aplica para los hacker novatos y mejor aun si tenemos vecinos que no usen seguridad, creando un escenario donde los más factibles de ser atacados son aquellos que no tienen ninguna medida de seguridad.

WEP y otros métodos de encriptación de equipo inalámbrico operan estrictamente entre nuestra computadora Wi-Fi y nuestro punto de acceso Wi-Fi o gateway.

El protocolo WEP es incorporado como una parte del protocolo 802.11b. Actualmente el estándar solo llamado por WEP de 40 bit, algunos equipos ya disponen de WEP de 64 y 128 bits.

Para asegurar los datos, WEP usa el algoritmo RC4 para encriptar los paquetes de información como ellos son enviados desde el punto de acceso a la tarjeta de red inalámbrica. Este el mismo algoritmo usado en muchos otras aplicaciones de Internet, tales como SSL (secure sockets layer.)SSL es él más común de los protocolos usados por tiendas en línea para encriptar información de los usuarios enviada sobre Internet. Esto reduce el riesgo de que un hacker husmee la información de tarjeta de crédito de un usuario del cable y adiciona una capa de protección para el proceso de transacción.

6.9 Filtro de control acceso al medio (MAC)

Como una parte del estándar 802.11b, cada radio Wi-Fi tiene un número de control de acceso al medio (MAC) asignado por el fabricante. Para incrementar la seguridad de la red inalámbrica, es posible para el administrador de IT programar el punto de acceso Wi-Fi corporativo para aceptar solo las direcciones MAC seguras y filtrar todas las demás. La tabla de control de las direcciones MAC así creada trabaja como un "bloqueo de llamadas" en un teléfono, si una computadora con una MAC desconocida trata de hace contacto, el punto de acceso no lo permitirá.

Cuando, se programe todas las direcciones MAC autorizadas de los usuarios en el punto de acceso de la compañía puede ser una tarea ardua y pesada para una organización y puede consumir un tiempo considerable, pero para los entusiastas de la tecnología casera puede ser una tarea sencilla, dado él numero limitado de direcciones MAC a ingresar.

Es posible para un hacker dedicado, clonar una dirección MAC, interceptando una dirección MAC y entonces programándola en su computadora para ser usada en difusión.

Sin embargo, mientras que en teoría esto es una excelente manera de parar a los hackers el acceso a la red WLAN, hay defectos serios en los filtros de MAC. El problema con los filtros de MAC es que las direcciones MAC pueden ser clonadas al cambiar la configuración de la WNIC, esto debido a que existe software que permite alterar la dirección MAC.

Teniendo el poder de ajustar la dirección MAC, los fabricantes de equipo pueden proporcionar más herramientas a los administradores de redes, para mantener controlada su red. Sin embargo este incrementado poder de administración, puede también permitir a personas maliciosas justamente tener mucho control.

A pesar de esto, instalaciones de redes pequeñas, usan técnicas de filtraje de direcciones MAC como un método efectivo para prevenir el acceso no autorizado.

6.10 Control de la zona de radiación

Cuando una red inalámbrica es activa, este hace un broadcast de la señal de radio frecuencia. Esta señal es usada para transmitir los datos inalámbricos desde un punto de acceso a una WNIC y viceversa.

Cuando usamos ondas de radio, hay un rango limitado impuesto por la señal de los dispositivos. Debido a la interferencia de los diferentes obstáculos a través de los cuales pasa la señal de radio, incluyendo la luz de sol y el aire, la señal del punto de acceso de se debilita a medida que nos retiramos de este. Si pudiéramos ver esta señal, podríamos ver círculos que van deteriorando su señal con la distancia. Estos círculos con conocidos como la zona de radiación.

Para ilustrar esto podemos usar una computadora portátil, para empezar encendemos el punto de acceso y la WNIC en la computadora portátil, empezamos a caminar alrededor de punto de acceso y cada vez que terminemos un círculo completo empezamos a retirarnos del punto de acceso progresivamente con cada vuelta alrededor de este. Veremos en la computadora portátil como cae la señal

recibida por la WNIC desde el AP, si graficamos esto, podremos obtener la zona de radiación para este AP y su ubicación en particular.

En adición al hecho de que la zona de radiación puede extenderse más allá de los límites físicos de la oficina o la casa, las herramientas y tecnologías usadas por hackers pueden amplificar la señal. Usando antenas direccionales de alta ganancia un hacker puede estar incluso a una distancia de hasta 20 millas y poder acceder la red, esto significa que si nos vemos a través de la ventana, no podemos ver al posible hacker.

Afortunadamente hay algunos métodos con los cuales podemos controlar esta señal.

El primer método es poner el punto de acceso en un punto central del sitio de la oficina. Aunque esto puede ser obvio, muchos puntos de acceso son puestos en un cuarto externo próximo a la pared y peor cerca de una ventana.

Si hay la necesidad de instalar algunos puntos de acceso a lo largo de un espacio largo, tratemos de posicionarlos tan cerca del centro de la construcción, o tan lejos de los muros exteriores como sea posible.

En adición a la administración de la posición física del punto de acceso, podemos también controlar la señal enviada hacia el exterior desde el punto de acceso. Por ejemplo, si el punto de acceso tiene algún parámetro donde variar la potencia transmitida o a través de la adición de atenuadores (existen en el mercado atenuadores de diferentes valores en dB de atenuación y en diferentes tipos de conectores) a la salida de señal de RF. (Normalmente la salida de la señal de RF es a través de conectores SMA) En particular, podemos controlar la potencia de la señal, la cual determina que tal lejos puede viajar esta. También podemos controlar la dirección de la señal a través del posicionamiento de las antenas. Por ejemplo algunos puntos de acceso permiten deshabilitar alguna de sus antenas, o podemos utilizar antenas direccionales y no omnidireccionales para limitar la radiación de la señal solo hacia el punto donde queremos cubrir de radiación.

Estos métodos de controlar la zona de radiación deben de ser utilizados en conjunción con otros métodos para completar la seguridad de la WLAN.

6.11 Seguridad defensiva a través de DMZ

Una DMZ es una red donde uno de los puertos LAN actúa como una clase de buffer entre la red pública y la red segura propia del usuario o la empresa, instalada en las otras interfaces LAN.

La DMZ da acceso a los servicios requeridos desde la red externa y la red segura. Los servicios son típicamente servidores de HTTP y FTP para acceso publico, a través del uso de filtros de IP, se puede prohibir el acceso desde Internet a nuestra red segura mientras todavía se proporciona acceso a los servicios en la DMZ.

Una DMZ o zona desmilitarizada, es un concepto de protección. Una DMZ define donde poner el servidor y dispositivos que no requieren la protección de la red segura o que al mantener a los dispositivos como la red inalámbrica insegura fuera de la red segura, esto es en la DMZ permiten disminuir el riego de ataque a la red segura que hace acceso a Internet. En otras palabras un servidor de Web o servidor de mail es frecuentemente instalado enana DMZ. Esto permite a cualquier usuario de Internet, accesar la asignación de recursos en el servidor, pero si e servidor esta siendo comprometido, un hacker no podrá ser capaz de usar su propia computadora para buscar el resto de la red. Técnicamente, una DMZ es actualmente una pequeña red propia, separada del resto de la red y separada de Internet.

Un Firewall frecuentemente protege la DMZ de ataques externos, sin embargo debido a que el servidor debe comunicarse hacia el mundo exterior, el Firewall será configurado para ignorar muchos tipos de conexiones, aparte el servidor es frecuentemente configurado para ser accesible fácilmente por usuarios de red interna.

6.12 Firewalls

Los Firewalls pueden hacer aparecer a una red invisible desde el Internet, y ellos pueden bloquear el acceso a nuestros archivos y sistema a usuarios no autorizados e indeseables. Sistemas Firewalls en hardware y software, monitorean y controlan el flujo de los datos de entrada y salida en ambos sistemas, por cable o inalámbricos, en redes de empresas, oficinas y en casas. Ellos pueden ser puestos para interceptar, analizar y parar un amplio rango de intrusos y hackers de Internet.

Como las VPN, hay muchos tipos y niveles de tecnologías de Firewalls. Muchas soluciones de Firewalls son solo software, muchos otros son poderosas combinaciones de hardware y software. Algunos Gateway Wi-Fi y puntos de acceso proporcionan un Firewall inter construido en el mismo dispositivo. Pero si no lo disponen, la mayoría de los Gateway Wi-Fi incluyen capacidades de ruteo NAT que actúa como un Firewall básico, haciendo las computadoras de la red y sus datos invisibles frente a hackers escaneando y probando.

6.13 Redes privadas virtuales (VPN)

La mayoría de las corporaciones, hoy en día, usan VPN para proteger sus conexiones remotas. Trabaja creando un "túnel" virtual seguro desde la computadora de un usuario hasta el punto de acceso o Gateway de otro usuario, a través de Internet. También trabaja para redes inalámbricas y puede efectivamente protegiendo la transmisión desde un equipo Wi-Fi y hacia los sistemas y servidores corporativos.

Una VPN trabaja a través de un servidor de VPN en la compañía, creando esquemas encriptación para la transferencia de datos hacia las computadoras fuera de las oficinas corporativas. El software especial para VPN en la computadora remota usa el mismo esquema de encriptación, habilitando a los datos para ser transferidos de forma segura hacia y desde las computadoras remotas sin oportunidad de intercepción.

Administradores de IT pueden establecer una VPN para soportar comunicaciones profesionales móvil desde aeropuertos o hoteles y trabajadores remotes trabajando desde sus casas, tan bien como las computadoras por cable o inalámbricas localizadas dentro de la compañía.

En los sitios de la corporación, las compañías pueden proporcionar seguridad y permitir abrir el acceso hacia el Internet y el correo para invitados proporcionando individual nivel de acceso a quien necesite acceder la red. Visitantes de la compañía, también como los trabajadores móviles, pueden acceder al Internet y hacer uso de los protocolos de correo. Sin embargo, los accesos VPN, los cuales permiten el acceso a la red de la corporación, a los sistemas de comunicación y correo corporativo, son proporcionados solo a quien ha sido autorizado.

Hay diferentes tipos y niveles de tecnologías de VPN, algunos de los cuales son muy costosos e incluyen hardware y software. Sin embargo, Microsoft proporciona tecnología de VPN gratis pero básica. Con sus sistemas operativos de servidores avanzados.

Usando VPN en adición con WEP, un hacker deberá de des-cifrar los datos dos veces. La primera capa es la encriptación WEP, y la segunda capa es la robusta encriptación de la VPN, debido a que un hacker no puede reproducir fácilmente el password de la VPN, certificados o claves de tarjetas inteligentes, los actos de ataques son mínimos en este tipo de combinación de seguridad.

Usando WEP y VPN en un punto de acceso apropiadamente configurado, puede afectar la velocidad de transmisión y la entrega de datos hasta en un 80 %. En otras palabras, tomara 10 minutos enviar un archivo con protección WEP y VPN, pero solo tomara 2 minutos sin encriptación.

Las VPNs crean un canal encriptado para proteger la comunicación privada sobre una red pública. Las soluciones de VPN requieren de una combinación de túneles de encriptación, autenticación y control de acceso.

Características clave de una VPN:

Encripta trafico entre dos puntos o dos enteras redes.

Basados usualmente en software

Proporciona varios niveles de encriptación limitado por restricciones de exportación.

Facilita comunicación segura fácil entre oficinas.

Proporciona acceso no caro a usuarios móviles.

Proporciona acceso completo a la red para los usuarios remotos.

Una VPN es útil para conectar un dispositivo móvil como una notebook o una PDA viajando alrededor del mundo y estos necesitamos accesar a la red de la compañía, esto a través de conexiones sobre Internet. Lo mismo aplica para empresas trasnacionales con oficinas alrededor del mundo y estas conectadas a la matriz sobre Internet usando VPN.

VPN proporciona seguridad, encriptando la comunicación de dos maneras:

Usuario-red (modelo de acceso remoto)- en esta configuración, los clientes remotos pueden conectarse a través de redes públicas como Internet. Usando VPN, los clientes remotos pueden ser parte de la red de la compañía.

Red-red (modelo sitio a sitio)- en esta configuración, una red de una oficina de una sucursal puede conectarse a través de una red publica como Internet, a otra rede de una oficina de otra sucursal. Esta configuración elimina la necesidad de una costosa red de área amplia (WAN).

6.13.1 Túneles

Envolviendo paquetes dentro de otros paquetes para protegerlos en su viaje, los túneles pueden proporcionar las siguientes características:

Enmascara direcciones privadas- las IP dentro de una organización frecuentemente de las de Internet. Los túneles ocultan las direcciones IP privadas durante su entrega a través de una red pública.

Transporte- permite en transporte de trafico no IP (como IPX o Apple talk). Aunque es el trafico IP el que domina el entorno de comunicación con su versión IPv4, ahora existe la posibilidad de usar IPv6 que es una mejora de la anterior.

Seguridad- los túneles pueden proporcionar seguridad adicional tales como encriptación, autenticación. Años atrás muchas compañías contrataban servicios de líneas privadas a las compañías de telecomunicaciones para poder conectar sus oficinas remotas con su corporativo, con la llegada de la seguridad y nuevas técnicas de encriptación y autenticación, ahora las compañías tienen la opción de poder llevar su trafico de voz y datos a través de redes publicas como el Internet sin sacrificar su seguridad ya que los túneles permiten mantener la información de una empresa o de una persona de manera encriptada imposibilitando a otros la lectura de la información así encriptada solo el origen y el destino del túnel podrán reconocer adecuadamente la información, por lo que permitiría a una empresa reducir sus gastos de telecomunicaciones al no tener que contratar enlaces dedicados como DS0 o E1, sustituyendo estos con conexiones de Internet ya sea con líneas telefonías POTS y ADSL

6.13.2 IPsec

IPsec es un protocolo diseñado para proporcionar seguridad criptográfica para los protocolos IPv4 e IPv6. IPsec se puede usar para establecer una transmisión de datagramas IP entre dos nodos IP. Los servicios de seguridad de IPsec incluyen el control de acceso, la integridad en la comunicación no orientada a conexión, la

autenticación del origen de los datos, protección contra reutilización, confidencialidad (cifrado) y confidencialidad de flujo de de trafico limitado. Debido a que estos servicios se proporcionan en el nivel IP, se pueden utilizar para ofrecer protección para IP y para los protocolos superiores como TCP, UDP, ICMP, OSPF y BGP.

IPsec implementa su seguridad utilizando dos protocolos de seguridad adicionales:

1. AH

2. ESP

IPsec también utiliza procedimientos y protocolos de gestión de claves criptográficas. El objetivo de IPsec es no afectar adversamente a los usuarios, host y demás componentes de Internet que no utilizan mecanismos de seguridad. Los mecanismos de IPsec están diseñados para ser independientes de los algoritmos lo que significa que se pueden utilizar sin afectar a otras partes de la implementación de IPsec. Se ha especificado un conjunto de estándares de algoritmos por defecto para facilitar la interoperabilidad global de Internet. El uso de algoritmos comunes junto con protocolos de administración de claves y protección del trafico IPsec pueden hacer mas segura la comunicación en el nivel IP.

Una implementación IPsec opera en un host, ruteador o puerta de enlace y protege el tráfico IP: la protección esta basada en directivas definidas en una base de datos de directivas de seguridad (SPD). La SPD es creada y mantenida por un usuario o administrador del sistema o por una aplicación que requiera aspectos de seguridad especiales.

6.13.3 Funcionamiento de IPsec

El encabezado de autenticación (AH) de IP proporciona integridad en la comunicación no orientada a conexión, la autenticación del origen de los datos y servicios óptimos anti-reutilización. E protocolo ESP proporciona confidencialidad (cifrado de datos) y confidencialidad de flujo de tráfico limitado. También proporciona

integridad en la comunicación sin conexión, autenticación del origen de los datos y servicio anti-reutilización. Tanto AH como ESP son mecanismos para controlar el acceso, que se basan en la distribución de claves criptográficas y la gestión del tráfico.

La seguridad del protocolo de Internet (IPsec) ha emergido como la principal suite de protocolos que gobiernan el uso de VPNs. IPsec entrega a nivel maquina autenticación y encriptación para VPN basadas en L2TP (protocolo de túnel de capa dos). IPsec proporciona integridad, protección y autenticación y opcionalmente privacidad y repetición de los servicios de protección. Los paquetes de IPsec comprenden los siguientes tipos:

Protocolo IP 50 – Este tipo de formato de encapsulamiento y seguridad de la carga. (ESP) Este define la privacidad, autenticación e integridad.

Protocolo IP 51 – Este es el formato de encabezado de autenticación. Define la autenticación y la integridad pero no la privacidad.

IPsec usa encriptación basada en DES (estándar de encriptación segura), el cual es de 56 bits o 3DES (triple DES), el cual es de 3 X56 o 168 bits. IPsec puede trabajar en dos modos: modo transporte o modo de túnel. El modo de transporte asegura un paquete IP existente desde la fuente hasta su destino, mientras que el modo túnel pone los paquetes en un nuevo paquete de IP que es enviado al final de túnel en el formato de IPsec. Ambos modos permiten encapsulación en los encabezados ESP o AH.

6.13.4 L2TP

El protocolo de túnel de capas 2 (L2TP) es el principal protocolo para implantaciones de capa 2 de VPN. Es el resultado de la combinación de los estándares L2F y PPTP.

6.13.5 L2F

Cisco originalmente desarrollo L2F como un mecanismo para configuración de túneles encapsulados UDP. Con el tiempo L2F fue popular como protocolo de túnel para VPN con sus propios derechos.

6.13.6 PPTP

El protocolo de túnel punto-punto (PPTP) es un protocolo de Microsoft para VPN. Este fue diseñado para proporcionar autenticación y encriptar las comunicaciones sin el requerimiento de la infraestructura de claves públicas. PPTP usa conexiones TCP para mantener el túnel y encapsulación de ruteo genérica (GRE) encapsula los frames de PPP para poner los datos en un túnel. Como un protocolo de VPN, PPTP perdió terreno por la popularidad del estándar IPsec.

6.13.7 PPP

PPP define un mecanismo de encapsulación para transportar paquetes multi-protocolo a través de la capa 2, enlaces punto a punto. Típicamente un usuario obtiene conexiones L2 a un servidor de acceso a la red (NAS) usando una de las numerosas técnicas (dial-up POTS, ISDN, ADSL, etc.) y entonces se ejecuta PPP sobre esta conexión. El punto de terminación L2 y la sesión PPP reside en el mismo dispositivo físico.

6.13.8 L2TP

L2TP extiende el modelo PPP a través de permitir a los puntos finales L2 y PPP residir en diferentes dispositivos interconectados por una red de conmutación de paquetes. Con L2TP un usuario tiene una conexión L2 a un concentrador de acceso (por ejemplo un banco de modems analógicos a digitales ADLS). El concentrador entonces hace túneles individuales de los frames PPP hacia el servidor de acceso de red. Este segrega el procedimiento cargado del los paquetes PPP desde la terminación de el circuito L2.

6.14 Autenticación y autorización RADIUS

RADIUS (servicios de marcado de acceso remoto) es otro método de tecnología estándar que es ya usada en la mayoría de las corporaciones para proteger el acceso a las redes inalámbricas. RADIUS es un esquema de nombre de usuario y contraseña que permite solo a los usuarios aprobados hacer acceso a la red, no afecta o encripta los datos. La primera vez que un usuario quiere acceder la red, archivos seguros o sitios de la red, el usuario debe ingresar su nombre y contraseña y enviarlo sobre la red a un servidor RADIUS. El servidor entonces verifica que el individuo tiene una cuenta y, solo así, asegura que la persona usa una contraseña correcta antes de que el usuario pueda entrar en la red.

RADIUS puede ser configurado para proporcionar diferentes niveles o clases de acceso. Por ejemplo, un nivel puede proporcionar acceso a Internet, otro puede proporcionar acceso a Internet también como a la comunicación de email. Todavía otra clase de cuenta puede proporcionar acceso a la red, email y a un servidor de archivos de negocios seguros.

Como otras tecnologías de seguridad sofistificadas ya mencionadas, RADIUS viene en una variedad de tipos y niveles, podemos hacer uso del RADIUS proporcionado por Microsoft en sus sistemas operativos de servidor avanzado, o podemos hacer uso de soluciones sofistificados con hardware y software.

6.15 TKIP

El protocolo de integridad de clave temporal (TKIP) es la más reciente característica de seguridad ofrecida por varios fabricantes para corregir la debilidad de WEP.

Este nuevo protocolo también usa RC4 como algoritmo de encriptación, pero remueve la debilidad del problema de la clave y cambia una clave nueva para ser generada cada 10 000 paquetes o 10 Kb, dependiendo de la fuente. En adición, elimina sus líos de los valores del vector de inicialización que son enviados como texto plano en la versión de WEP. Esto significa que ahora el IV (vector de

inicialización) es encriptado. También incluido en TKIP un método mas seguro y robusto para verificar la integridad de los datos, llamado el chequeo de integridad de mensaje, esta parte de TKIP cierra un agujero que permitía a los hacker inyectar datos en los paquetes, y así ellos podían deducir más fácilmente la clave de flujo usada para encriptar los datos.

6.16 AES

Estándar de encriptación avanzada (AES) es un nuevo método de encriptación que fue seleccionado por el gobierno de los Estados Unidos para remplazar a DES como su estándar, es bastante robusto y esta actualmente bajo revisión para la siguiente versión de Wireless 802.11 (802.11i)

AES usa un algoritmo conocido como Rijndael. El algoritmo fue ideado por Joan Daemen y Vincent Rijmen y ahora es parte de AES seleccionado de un proceso que tomo el mejor algoritmo propuesto como esquema para el sector publico.

Este evento de selección del mejor algoritmo fue a causa del rompimiento de la encriptación previa (DES) que fue rota en 1990.

La fortaleza de AES ha sido probada, hay tres opciones, debido a que AES permite diferentes tamaños de claves, dependiendo de las necesidades. El tamaño de la clave refleja la fortaleza de la encriptación así como también la cantidad de procesamiento requerido para encriptar y descifrar el texto.

3.4×10^{38} claves de 128 bit posibles

6.2×10^{57} claves de 192 bit posibles

1.1×10^{77} claves de 256 bit posibles

En otras palabras usando la misma tecnología para descifrar DES, tomaría 149 trillones de años para descifrar AES, el hecho es de que AES es un muy buen

algoritmo y se espera que sea el estándar por muchas décadas por venir. Como cualquier algoritmo de encriptación, AES será descifrado eventualmente.

AES tiene mas sobrecarga que RC4. Esto es debido al procesamiento extra requerido durante el proceso de encriptación y des-encriptación, que es más complejo en relación al relativamente simple RC4. Para ilustrar esto, el algoritmo RC4 es frecuentemente codificado en alrededor de 50 líneas de código, mientras AES toma alrededor de 350 líneas. Aunque esto hace que AES acapare recursos de procesamiento del CPU, existe hardware que acelera el rendimiento de la encriptación para compensar y evitar sobre cargar el proceso de encriptación al Cpu principal.

6.17 SSL

Capa de conexión segura (secure socket layer) es un protocolo que ha sido usado por años en sistemas en línea es la más popular forma de aplicar el uso de encriptación CR4 antes de enviar datos sobre el Internet, este proporciona una capa de seguridad a cualquier dato sensitivo. Cualquier desde almacenes en el Web, bancos en línea, sitios de email basados en Web y más usan SSL para mantener seguros los datos. La razón por la cual SSL es importante, es debido a que sin encriptación cualquiera con acceso, puede husmear y leer la información como texto plano.

Cuando construimos una WLAN segura, uno de las más importantes y necesarias partes es la autenticación. Aunque hay algo de protección con password compartido que es usado para configurar WEP, este solo encripta los datos. El defecto de esto es que el sistema asume que el usuario se le permite enviar datos si el password compartido es el correcto.

Aunque la autenticación es importante y necesaria, es también potencialmente vulnerable a algunos tipos de ataques. Por ejemplo los sistemas de autenticación de usuarios asumen que la persona que envía el password es efectivamente el dueño de la cuenta, que puede no ser del todo cierto. Otra debilidad es que la información

es enviada del cliente hacia el sistema host, por lo tanto la información de autenticación puede ser husmeada, por lo cual es importante SSL para la autenticación de usuarios.

6.18 IDs (detección de intrusión)

Los sistemas de detección de intrusiones son a las redes de computadoras como las alarmas de ladrones a las casas. El mejor sitio para poner un ID es detrás de un Firewall, de esta manera la cantidad de trafico que es revisado es menor, reduciendo en numero de falsas alarmas.

Los sistemas de IDs, basados en el monitoreo de archivo de registro (Log file) monitorean del archivo de Log (actividad de la red), intenta detectar intrusiones a través de la búsqueda en este archivo de información que lo conduzca a la determinación de una intrusión a la red, cuando a detectado la intrusión realiza una acción como imprimir un mensaje, enviar un correo electrónico, etc. Existe también IDs basados en monitores de integridad que observan la estructura de sistema para ver si hay cambios realizados por intrusos entre los atributos que se monitorean están:

1. archivos adicionados, borrados o modificados.
2. banderas de archivos (oculto, solo lectura, archivo, etc.)
3. ultima fecha de acceso.
4. ultima fecha de escritura
5. fecha de creación
6. tamaño de archivo

6.19 Kerberos

Otra manera de proteger los datos inalámbricos es usando una tecnología llamada Kerberos creada por el MIT (Instituto Tecnológico de Massachussets). Kerberos es un sistema de autenticación de red sin confianza basado en la distribución de claves. El objetivo de Kerberos, tal y como se implemento originalmente, fue ofrecer un

medio seguro de autenticación para un gran numero de estaciones de trabajo publicas. Permite a las entidades comunicarse sobre una red alambrada o inalámbrica para proporcionar su identidad a cada uno de los demás mientras previene el ser escuchados o se repiten ataques a esta. También proporciona integridad al flujo de los datos (detección y modificación) y recrecía (previene lecturas no autorizadas) usando sistemas de encriptación tales como DES.

Después de que el cliente y el servidor han usado Kerberos para proveer su identidad, ellos pueden también encriptar toda su comunicación para asegurar la privacidad e integridad de los datos como ellos van en sus empresas.

Kerberos trabaja proporcionando principalmente (a usuarios o servicios) etiquetas digitales que ellos pueden usar para identificar ellos mismos en la red y claves criptográficas secretas para asegurar la comunicación. Una etiqueta es una secuencia de unos pocos cientos de Bytes que pueden ser montados en virtualmente cualquier otro protocolo de red.

El acceso a un servicio no se otorga automáticamente, en primer lugar se autentica al cliente para determinar si el acceso esta o no permitido al cliente. Los dos componentes más importantes que implementa Kerberos son le servidor Kerberos y el servicio de concesión de vales (TGS) El uso de estos componentes se explica a continuación:

El cliente que desea hacer uso de un servicio contacta en primer lugar con el servidor de Kerberos con una petición para obtener una etiqueta para ser utilizado con el servicio de concesión de tiquete (TGS) el TGS se conoce como centro de distribución de claves (KDC) en Windows 2000.

El servidor devuelve un tiquete TGS cifrado con la contraseña del usuario. Si el usuario introduce una contraseña correcta, el tiquete es descifrado para obtener tiquetes del TGS para diferentes servicios.

El cliente envía una petición una petición al KDC para obtener un tiquete para un servicio como Telnet, para un host particular. Dentro de este mensaje se encuentra el tiquete Kerberos que establece la identidad del cliente. El mensaje se cifra utilizando una clave de sesión incluida en el tiquete TGS enviado al cliente en el paso 2.

El KDC devuelve un tiquete de sesión para utilizarlo entre el cliente y el servicio, así como un tiquete usado para que el servidor compruebe que el cliente esta autorizado para utilizar ese servicio.

Antes de utilizar cualquier servicio, debe obtenerse un TGS. Este se obtiene cuando el usuario envía una petición inicial al servidor Kerberos. La petición inicial para obtener el tiquete TGS sé envía de forma transparente cuando el usuario entra en la red. El servidor responde a la petición inicial con un tiquete cifrado con la contraseña del usuario. Si el usuario introduce la contraseña correcta, el tiquete puede ser descifrado y utilizado para obtener el acceso a los servicios. Debido a que la contraseña no abandona la maquina del cliente (solo sé envía una versión modificada con una función de dispersión de la contraseña), no se compromete su seguridad por ser transmitida por la red. El tiquete TGS es valido durante una cantidad de tiempo limitada (10 horas por defecto, lo cual de controla modificando las directivas de seguridad de Kerberos)

Kerberos proporciona un mecanismo de autenticación que demuestra la identidad del cliente que hace una petición para un servicio. Esto es, Kerberos determina si el cliente es quien dice ser. Después de completada la autenticación la siguiente etapa es la autorizar al cliente a utilizar un servicio. Kerberos no realiza la autorización, la realizan los servidores en los que se ejecutan los servicios.

El nombre de Kerberos deriva de la mitología griega y es el nombre de un perro de tres cabezas que guarda las puertas a Hades.

Kerberos es disponible gratis por el MIT y como un producto desde muchos diferentes proveedores.

6.20 Infraestructura de claves publicas inalámbrica PKI

La infraestructura de claves publicas es un sistema de certificados digitales, autoridades de certificación otras autoridades de registro que verifican y autentifican la validez de cada parte involucrada en transacciones electrónicas a través del uso de criptografía de claves publicas.

En la criptografía de claves publicas, la encriptación y des-encriptación son diferentes. Esto es en contraste con la criptografía de claves simétricas, donde un a sola clave es usada para ambos procesos, encriptación y des-encriptación. En la encriptación de claves publicas, cada usuario tiene un par de claves, conocidas como clave publica y clave privada.

6.20.1 Algoritmos de claves publicas comunes

Los algoritmos de encriptación utilizados mas comúnmente el los mecanismos de de claves publicas son una parte importante en la seguridad de los sistemas de autenticación por claves publicas. Los siguientes son algunos de los más comúnmente usados y probados en algoritmos de claves públicas:

1. RSA, el algoritmo es nombrado debido a sus inventores Ron Rivest, Adi Shamir y Leonard Adleman. Es actualmente el más comúnmente usado en algoritmos de claves públicas. RSA es criptográficamente fuerte y esta basado en la dificultad de factorizar números largos. RSA es también debido a que es capaz de hacer operación de firmas digitales y operación de intercambio de claves.
2. DSA, La agencia de seguridad nacional de los estados unidos (NSA) invento el DSA (algoritmo de firma digital). Este algoritmo puede ser usado para operaciones de firmas digitales, pero no para encriptación de datos. La fuerza de la encriptación esta basada en la dificultad de calcular algoritmos discretos.

3. Diffie Hellman, nombrada en honor a sus inventores Whitfield Diffie y Martin Hellman. Este algoritmo puede ser usado solo para el intercambio de claves. La fuerza de la encriptación esta basada en la dificultad para calcular algoritmo discretos en campos finitos.

Las firmas digitales confían de funciones matemáticas llamadas lió de una vía. Un lió difiere de de la criptografía basada en claves. Los líos utilizan funciones matemáticas de una sola vía (irreversibles) para transformar datos en resumen de longitud fija, conocidos como los valores de lió. Cada valor de lió es único, así la autenticación usando los valores de lió es similar a utilizar las huellas digitales. Para verificar el origen de los datos, un recipiente puede des-encriptar el valor de lió original y compararlo con un segundo valor de lió generado desde el mensaje recibido.

6.20.2 Autoridades de certificación

Una autoridad de certificación (CA) es cualquier entidad o servicio que emite certificados. Los CAs actúan como garantizadores del contrato entre las claves públicas y la identidad propia de la información que es contenida en el certificado que es emitido.

Cuando se usa PKI para comunicaciones comerciales con organizaciones exteriores, muchas compañías contratan los servicios de un CA comercial tales como VeriSign. Los precios varían dependiendo del nivel de encriptación del servicio que se contrate.

6.20.3 Revocación

Los certificados son emitidos por un periodo valido esperado. Sin embargo bajo ciertas circunstancias puede suceder que un certificado sea invalidado antes de su fecha de expiración. Por ejemplo, si hay un conocido compromiso de una correspondiente clave publica, el CA tendrá la necesidad de revocar el certificado. El estándar X.509 proporciona mecanismo s para esta revocación. Esto requiere que

cada CA periódicamente emita una estructura de datos firmada llamada lista de revocación de certificados (CRL). El CRL es una estampa de tiempo de lista de certificados inválidos o robados que han sido revocados. El número de serie del certificado revocado es usado para ser identificado en el CRL.

Los CAs emiten nuevos CRLs de manera regular, los cuales pueden ser en horas, días o semanas. Una ventaja de estas revocaciones es que los CRLs pueden ser distribuidos a través del mismo canal como los certificados mismos.

Capitulo 7 Organismos WLAN

7.1 Organismos internacionales.

Los organismos involucrados en el desarrollo de estándares y tecnologías son organismos de científicos, ingenieros y demás personal técnico asociado al área de las telecomunicaciones e informática, su función es establecer estándares, recomendación, etc. que permitan la inter-operatibilidad de los dispositivos de comunicaciones e informática.

7.1.1 Organización Internacional para la estandarización

La Organización Internacional para la Estandarización (ISO) es una confederación a través del mundo de cuerpos nacionales de normas, con cerca de 100 países. ISO es una organización no gubernamental establecida en 1947. La misión de ISO está promocionar el desarrollo de Estandarización y relacionar las actividades en el mundo con una vista para facilitar el cambio internacional de mercaderías y servicios, y a la cooperación creciente en las esferas de actividad intelectual, científica, tecnológica y económica. Los desarrollos de ISO son el trabajo resultante en los acuerdos internacionales que se publican como las Normas Internacionales.

7.1.2 Comisión Internacional Electrotécnica.

El objeto de la Comisión está promocionar cooperación internacional - sobre todas las preguntas de estandarización y relacionar las materias en los campos de ingeniería eléctrica y electrónica y así para promocionar comprensión internacional.

El IEC se compone de Comités Nacionales, de los que hay 49 en la actualidad, representando todos los países industriales en el mundo.

7.1.3 Unión Internacional de Telecomunicaciones.

El ITU es una organización intergubernamental, dentro del cual los sectores públicos y privados colaboran para el desarrollo de telecomunicaciones. El ITU adopta los tratados y regulaciones internacionales gobernando todo uso terrestre y de espacio del espectro de frecuencia así como también el uso de la órbita de satélite geoestacionaria, También desarrolla normas para facilitar la interconexión de sistemas de telecomunicación sobre una escala a través del mundo sin considerar el tipo de tecnología usó.

7.1.4 Fuerza de tarea de Ingeniería Internet.

El Internet que Diseña e (IETF) es el desarrollo e ingeniería de protocolo brazo del Internet. El IETF es una comunidad internacional abierta grande de diseñadores de red, operador, vendedores, y los investigadores, concernieron con la evolución del Internet de arquitectura y la operación lisa del Internet. Es abierto a cualquier individuo interesado. El trabajo técnico real del IETF sé a hecho en sus grupos de trabajo, que son organizado por el tema en varias áreas p. Ej. , Desarrollando la gestión de red, seguridad, etc.

7.1.5 Instituto de Ingenieros Eléctricos y Electrónicos.

El Instituto de Eléctrica y Electrónica (IEEE) es en mundo la sociedad profesional técnica más grande. Fundada en 1884 por un puñado de profesionales de la nueva disciplina ingeniería eléctrica, la Institución de hoy está comprendida de más de 320,000 miembros quien conduce y participa en sus actividades en 147 países. Los hombres y las mujeres del IEEE son los profesionales técnicos y científicos que hacen los adelantos de ingeniería. Los objetivos técnicos del IEEE enfocan en avanzar la teoría y práctica de eléctrica, electrónica y computadora e ingeniería de computadora ciencia. Para dar cuenta estos objetivos, el IEEE patrocina conferencias técnicas, simposium y reuniones locales a través del mundo: publica aproximadamente 25% de los papeles técnicos de mundo en eléctrico, electrónica y la computadora; provee programas educativos para guardar conocimiento de sus miembros y pericias de estado del arte. El propósito de todas estas actividades es: (1) para mejorar la calidad de vida para todos los pueblos mediante la conciencia pública mejorada de las influencias y aplicaciones de sus tecnologías; y (2) para avanzar la posición de la profesión de ingeniería y sus miembros.

7.1.6 Instituto de estándares en telecomunicaciones de Europa

Subcomité de HIPERLAN. La más joven de las tres normas Europeas que hacen cuerpos, reconocida por el Consejo Europeo de Ministros por la Directiva de Consejo 83/189, (ETSI) se estableció en 1988 para colocar normas para Europa en telecomunicaciones y, en cooperación con la Unión Europea de Broadcasting (EBU) y CEN/CENELEC respectivamente.

ETSI es un foro, la única en el área de telecomunicaciones, que reúne todos los personajes clave, operador de red, proveedores de servicio, fabricantes, administraciones, usuarios y la comunidad de investigación. Solo dentro de ETSI hay un foro único que puede tomar una descripción de los requerimientos de mercado para la estandarización con base en un consenso genuino. Además, los sistemas abiertos son vitales para la construcción de la infraestructura de la Sociedad de Información, la franqueza es una característica importante de las actividades de estandarización del ETSI.

La ETSI tiene como misión:

Como el cuerpo de normas de telecomunicaciones, oficialmente reconocido por la Unión Europea, apunta para ser el mejor proveedor de especificaciones técnicas voluntarias en la Europa.

7.1.7 IEEE 802.11, Grupo De trabajo para redes de computadoras local Inalámbricas

El IEEE 802.11 Grupo De trabajo trabaja sobre una norma para inalámbrica LAN's. La norma propuesta provee conectividad inalámbrica a la maquinaria automática, equipo, o estaciones que requieren despliegue rápido, ser portátil, o sostenido a mano, o que puede montarse sobre vehículos rápidamente móviles dentro de un área local. El IEEE 802.11 Grupo De trabajo ofrece una norma para el uso por cuerpos reguladores para normalizar acceso a uno o más frecuencia agrupa a objeto de comunicaciones locales de área.

7.1.8 Consorcio inalámbrico

La Universidad de Nuevo Hampshire Laboratorio de Interoperabilidad de (IOL) anda metido en el trabajo de investigación y desarrollo.

El Consorcio Inalámbrico prueba productos y software 802.11 ambos desde una perspectiva de interoperabilidad y de conformidad.

El Consorcio Inalámbrico se formó en Marzo de 1996 y es uno de ocho consorcios de la Universidad de Nueva Hampshire Laboratorio interoperabilidad IOL. El Consorcio se formó mediante el acuerdo cooperativo de vendedores interesado en probar productos Inalámbricos 802.11. Los miembros Inalámbricos de Consorcio acuerdan guardar un foco técnico, y cubrir los costos de pruebas crecientes.

7.1.9 Asociación de comunicaciones y computadoras portátiles

La Asociación de Comunicaciones y computadora portátil se fundó para proveer un foro para permitir industrias dispares, aprender sobre el uno al otro, y colaborar sobre el casamiento de estas industrias. Los desafíos que rodean la implementación de movilidad cierta son complejos.

El PCCA es una organización sin fines de lucro formada para proveer un foro para todas las compañías y los individuos interesados en interoperabilidad de cómputo móvil y comunicaciones. El propósito del PCCA está permitir, desarrollar, y promocionar la adopción de normas y software para interoperabilidad de cómputo móvil y comunicaciones.

Los miembros incluyen representantes desde:

Los Suministradores de Información.

Las Proveedores de comunicaciones.

Los Fabricantes de Equipo de Comunicaciones.

Los Vendedores de Equipo de Comunicaciones.

Los Fabricantes de Equipo de Computadora.

Los Vendedores de Equipo de Computadora.

Los vendedores de Sistemas.

Los Vendedores de Software.

Los Revendedores de valor agregado.

Otros canales de distribución.

Otros Asociaciones.

Implementadores.

Los Usuarios Individuales.

Otros Partidos Interesados.

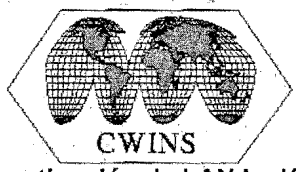
7.1.10 LAN inalámbrico Alianza (WLANA)

El LAN el Inalámbrico Alianza (WLANA) es una asociación de industria que provee conciencia y crea excitación sobre las capacidades actuales y futuras direcciones de redes de computadoras local inalámbricas. La Alianza se formó con respecto al interés aumentado en datos inalámbricos desde ambos clientes y los medios. Los vendedores de LAN inalámbrico reconocieron que había un número creciente de clientes potenciales con datos inalámbricos. Los miembros proveen educación en proceso sobre capacidades actuales, aplicaciones específicas, y futuras posibilidades de LANS inalámbrico. El WLANA se compromete para establecer LANS inalámbrico como un componente clave de tecnología de red de computadoras local.

El corazón de la misión de WLANA esta en educar clientes existentes y potenciales, vendedores de software, y consultores de sistema en una variedad de industrias sobre los beneficios de la tecnología LAN inalámbrico.

7.1.11 Foro de interoperabilidad de LAN inalámbrico.

Un grupo de proveedores de productos de computo móvil y servicio han formado el Foro de interoperabilidad de LAN inalámbrico(Foro WLI) cuyas compañías miembro entregarán una gama amplia de redes de área local inalámbrica (LAN), productos y servicios, promocionando el crecimiento del LAN inalámbrico en el mercado. El foro de WLI ha publicado una especificación de interfaz abierta permite a las partes independientes desarrollar productos compatibles, y han establecido una certificación para la interoperabilidad de productos LAN inalámbrico.



7.1.12 Laboratorio de investigación de LAN inalámbrico

El Laboratorio de Investigación de LAN´s Inalámbrico (WLRL) se estableció dentro del Centro de Información Inalámbrica de Red para el Estudio (CWINS) en Worcester Polytechnic Institue (WPI), en Worcester, Massachusetts. WPI y CWINS tienen historias largas de innovación y la excelencia técnica y educativa, representa la mejor alternativa para establecer un creíble y técnicamente capaz recurso.

Los objetivos claves del WLRL son:

Sirva como un punto focal para tecnología LAN inalámbrico.

Especifica y desarrolla pruebas clave y criterios de referencia, software, así como también compatibilidad, interoperabilidad, y normas, sistemas y software de comprobación.

Diseña y desarrolla planificación de instalación, simulación, y depura herramientas ambos hardware y software.

Distribuye los resultados de actividades de centro, sujeto a la aprobación de los miembros asegura, en forma de artículos, presentaciones, conferencias, y una presencia sobre Internet.

7.1.13 Asociación de estándares IEEE

La asociación de estándares de la IEEE (IEEE-SA) es líder en el desarrollo de estándares industriales globales incluyendo

Energía y potencia	Biomédica y salud
Tecnología de la información	Telecomunicaciones
Transportación	Nanotecnología
Seguridad de la información	Baterías recargables para PC

Arquitectura para medios compartidos encriptados

Infraestructura para la emisión de claves publicas, emisión de certificados

y componentes de administración

El IEEE ha ofrecido un programa de desarrollo de estándares, en adición a producido el prominente estándar 802 para redes alambradas e inalámbricas de área local y metropolitanas. Cada año la IEEE-SA prospera debido a la diversidad técnica de sus más de 20000 participantes, consistiendo estos de líderes en tecnología de todo el globo incluyendo individuos en corporaciones, organizaciones, universidades y agencias de gobiernos.

7.1.14 Grupo de trabajo IEEE 802.16

El grupo de trabajo 802.16 en estándares de acceso inalámbrico de banda ancha, desarrolla estándares y recomienda prácticas para soportar el desarrollo e implementación de redes de área metropolitana inalámbricas de banda ancha .el 802.16 es la unidad del comité de estándares IEEE 802 LAN/WAN, el principal foro internacional para la estandarización de redes inalámbricas.

El IEEE 802.16, dirige la conexión de la primer/ultima milla en redes de are metropolitana, se enfoca en la eficiencia del uso del ancho de banda entre los 10 y los 66 GHz y la región de 2 a 11 GHz desde fines del 2002). Define la capa de control de acceso al medio (MAC) que soporta múltiples especificaciones de la capa física adaptadas para la banda de frecuencia en uso.

7.1.15 Grupo de trabajo IEEE 802.15 para redes inalámbricas de área personal

El 802.15 WPAN dirige su esfuerzo al desarrollo de estándares de consenso para redes de área personal o redes inalámbricas de distancia corta. Estas WPAN dirigen las redes inalámbricas de dispositivos de cómputo móvil y portátil, tales como PCs, DPA, periféricos, teléfonos celulares, pagers y electrónica de consumo; permitiendo a estos dispositivos comunicarse e ínter operar con otros. La meta es, publicar estándares, recomendar practicas o guías que tienen una amplia aplicación en le mercado para la interoperabilidad con soluciones de redes inalámbricas y

alambradas. El IEEE 802.15 es parte del comité de estándares de redes de área metropolitana y local 802.

7.1.16 Comité de estándares IEEE 802 LAN/MAN

El comete de estándares IEEE 802 LAN/MAN desarrolla estándares para redes de área local y estándares para redes de área metropolitana. El mas ampliamente usado es la familia Ethernet, Token Ring , wireless LAN, etc. Un grupo de trabajo individual proporciona atención en cada área.

7.1.17 Alianza Wi-Fi

La alianza Wi-Fi es una asociación internacional sin beneficio, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en las especificaciones IEEE 802.11. Actualmente la alianza Wi-Fi tiene más de 200 compañías miembros alrededor del mundo y más de 1000 productos han recibido la certificación Wi-Fi desde que empezó en marzo del 2000. La meta de los miembros de la alianza es aumentar la experiencia de los usuarios a través de la interoperabilidad de los productos.

Capitulo 8 Implementación de la red WLAN en la ENEP Aragón

8.1 Implementación de una red inalámbrica en la ENEP Aragón

La idea de implementar una red inalámbrica dentro de la ENEP Aragón obedece a la intención de brindar a los alumnos, nuevos mecanismos de acceso a la información disponible en Internet así como en la intranet de la propia escuela, incrementar los medios de comunicación entre toda la comunidad de estudiantes de la escuela y permitir que los estudiantes sean creativos al momento de estudiar utilizando tecnología de punta, esto permitirá a la escuela y a los alumnos mejorar el aprovechamiento de su espacios físicos y de tiempo, y que estos sean optimizados incrementando el desempeño de los estudiantes.

Ahora que tenemos todas las herramientas relacionadas con el despliegue de una red inalámbrica y viendo las ventajas que tiene el estándar 802.11g sobre los otros estándares, propongo los siguientes puntos para su instalación y uso en la ENEP Aragón, como son:

1. Propuesta para los sitios de instalación de los puntos de acceso.
2. Pruebas de monitoreo y supervisión del área de instalación.
3. Consideraciones de propagación y del estándar 802.11g.
4. Equipos WLAN y LAN propuesto para los puntos de acceso.
5. Interconexión de la red inalámbrica.
6. Interconexión a Internet.
7. Recomendaciones para el equipo de los clientes inalámbricos.
8. Cobertura de los puntos de acceso instalados.
9. Seguridad en la red inalámbrica.
10. Funciones de la administración.
11. Políticas de usuarios inalámbricos.
12. Análisis de costos

8.1.1 Propuesta para los sitios de instalación de los puntos de acceso

La instalación de los puntos de acceso debe estar en función de dos parámetros muy importantes, los cuales son: demanda de servicio y seguridad. Por el lado de la demanda considero en función de las actividades normales de un estudiante dentro de la escuela, que los alumnos pasamos bastante tiempo en los salones de clase tomando clase de cualquier materia, en la biblioteca investigando algún tema de tarea y en los pasillos discutiendo con los compañeros de cualquier tema, personal, familiar y escolar. Por lo que en función de la demanda tratare de cubrir estas áreas de alto trafico de alumnos, salones, biblioteca y áreas de transito (pasillos y explanadas). Cubriendo estas áreas podremos atender a un porcentaje muy elevado de la población estudiantil.

Siguiendo un principio básico de seguridad, que es, ubicar la red inalámbrica de manera que se encuentre limitada su propagación hacia el exterior de los limites físicos de la escuela, considerando la distribución de los edificios dentro de la ENEP Aragón, considero que los edificios pueden funcionar a manera de "muros" que limitan la salida de la señal de RF, creando zonas de confinamiento, ubicando a los puntos de acceso en las explanadas formadas por los edificios que las rodean. No son barreras perfectas para la señal de RF pero ayudan demasiado a contener la señal de RF dentro de ciertos límites. En algunos casos será necesario ubicar a los puntos de acceso al descubierto debido a que no hay más edificios para confinar la señal de RF dentro de las explanadas o estos edificios no encierran por completo a la señal, dejando huecos por donde la señal puede propagarse a mayor distancia pero es necesario esto para poder dar el servicio en algunos edificios, más sin embargo, la seguridad también será reforzada por la autenticación de WPA y sus protocolos de encriptación.

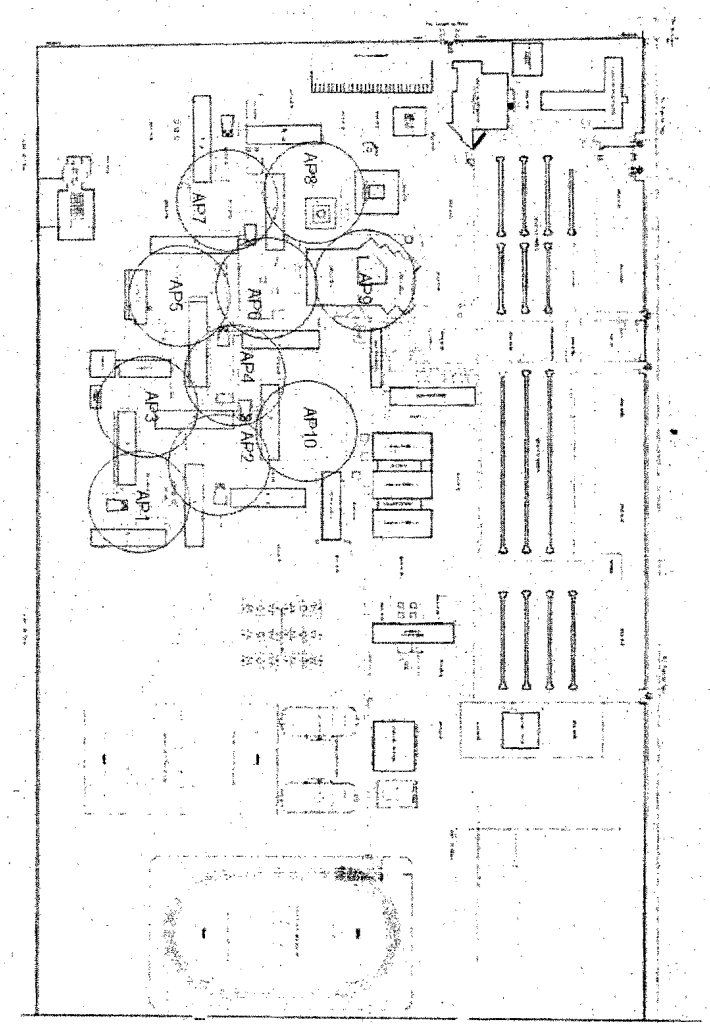


Figura 8.1.1-1 Diagrama de puntos de acceso

Por lo antes mencionado propongo la siguiente configuración de 10 puntos de acceso, tratando de cubrir las zonas de mayor demanda, esto es, salones de clases y la biblioteca, siendo cubiertas además las explanadas principales como se muestra en la. Figura 8.1.1-1 Diagrama de puntos de acceso. Como se ve en el diagrama mi propuesta es poner cada punto dentro de explanadas formadas por cuatro edificios, uno por cada lado. Esta configuración permitirá contener la señal de RF dentro de estas áreas.

Recordando los diferentes tipos de dispositivos WLAN, podemos sugerir que una vez que la red se encuentre instalada, podrá ser utilizada por:

1. computadoras portátiles con una tarjeta PCMCIA o USB WLAN
2. computadoras de escritorio con una tarjeta PCI o USB WLAN
3. Agendas portátiles (PDA) con una tarjeta CompactFlash card WLAN

Estos dispositivos podrán ser utilizados para conectarse a Internet, revisar el correo electrónico y bajar documentos de Internet y/o de la intranet de la escuela, así como aplicaciones de comunicaciones como mensajeros de texto o voz. Todo esto desde cualquier punto que sea cubierto por la zona de cobertura de la red WLAN.

Básicamente se puede considerar que los puntos de acceso estarán ubicados en las explanadas principales cubriendo áreas de transito, como pasillos, explanadas y en parte a los salones de clases, así como el edifico de la biblioteca. Beneficiando a alumnos y maestros que puedan y quieran hacer uso de este servicio. La escuela podrá definir un costo del servicio para poder financiar su mantenimiento y ampliación de nuevos servicios para hacer crecer a la red y aumentar el número de usuarios beneficiados.

8.1.2 Prueba de monitoreo y supervisión del área de instalación.

La supervisión nos proporciono valores de la señal de RF con los que podemos determinar las características de la propagación de la señal tanto dentro como fuera de los salones, para determinar la mejor estrategia de implementación de los sitios así como para determinar si la propuesta original se puede llevar a cabo o requiere modificaciones.

La instalación de la red inalámbrica requiere datos que nos permitan determinar por donde pasa la señal para saber que áreas son cubiertas y por donde no pasa la señal, para tener la seguridad de que los puntos de acceso con frecuencias iguales no se interfieren, para evitar que la señal de RF salga de los límites de la escuela así como evitar que se interfieran los puntos de acceso, esto como medida de seguridad de la propia red. Los obstáculos que en este caso en su mayoría son los edificios se utilizaran para contener la señal de RF. Debido a que el estándar 802.11g solo especifica tres frecuencias no traslapadas, me veo en la necesidad de hacer uso de la técnica de reutilización de frecuencia para incrementar el área de cobertura. Por lo tanto las pruebas se van a realizar considerando puntos de acceso que reutilizan los tres canales de frecuencias no traslapados.

Las pruebas de monitoreo se obtuvieron con el siguiente equipo WLAN:

Punto de acceso en la banda de 2.4 GHz (802.11g)	1
Computadora portátil con Windows XP	1
Tarjeta de red inalámbrica 802.11g PCMCIA	1
Software network stumbler versión 0.4.0	1
Batería portátil de 9 volts CD	1

A continuación muestro los valores obtenidos en las pruebas de monitoreo (survey) dentro de la ENEP Aragón.

8.1.3 Monitoreo con un punto de acceso dentro de un salón

Se hicieron mediciones de la señal de Rx dentro de los salones y fuera de estos, en las explanadas principales de la escuela, instalando de manera provisional puntos de acceso en estos lugares, se hicieron recorridos con un cliente WLAN y se anotaron los valores de recepción para su análisis. Los parámetros de prueba y sus resultados fueron los siguientes:

Los datos de la configuración de prueba fue la siguiente:

Se instalo un punto de acceso dentro del salón A-316 con la siguiente configuración:

Potencia de transmisión	Pt = 23 dBm (200 mW)
Ganancia de la antena omnidireccional	Gt = 2dBi
Altura de la antena:	H = 2 metros

Se utilizo un cliente WLAN con la siguiente configuración:

Ganancia de la antena de recepción:	2 dBi
Nivel de umbral de Rx (sensitividad mínima)	-92 dBm

Los resultados de las pruebas se muestran en la Tabla 8.1.3-1.

Sitio del punto del acceso: Salón A-316.

No	Sitio Monitoreado	Rx dBm	SNR dB	Ruido dBm	Ping
1	A-211	-86	14	-100	2 de 3
2	A-212	-91	9	-100	no
3	A-304	-86	14	-100	no
4	A-305	-80	24	-100	ok
5	A-306	-64	36	-100	ok
6	A-313	-80	20	-100	no
7	A-314	-67	23	-100	ok
8	A-315	-63	37	-100	ok
9	Interior del A-316	entre -35 y -52	entre 65 y 48	-100	ok
10	Afuera del A-316 a un Metro de distancia	-58	43	-100	ok
11	A-324	-76	24	-100	ok
12	A-325	-80	20	-100	no
13	A-411 al A-416	entre -87 y -92	<12	-100	no
14	Afuera de la biblioteca A 50 m del A-316	-92	8	-100	ok
15	Frente al edificio de gobierno a 60 m del A-316	-82	15	-100	ok
16	Frente a la biblioteca A 80 m del A-316	-92	8	-100	no
17	Frente al A-10	-87	10	-100	no

Tabla 8.1.3-1 Resultados del monitoreó dentro de salones

Estas fueron todas las pruebas realizadas dentro de los salones, los salones no marcados como el A-326 no se monitoreo debido a que este se encontraba cerrado en el momento de las prueba pero puede considerarse similar al valor obtenido en el

salón inferior que sería el A-306, si observamos básicamente la señal no viaja más allá de tres muros, y sus resultados puede ser utilizados como referencia de cómo se comportaría la señal si se instalaran otros puntos de acceso dentro de otros edificios, dado que estos comparten la misma configuración física, distribución y tamaño, también utilizan los mismos materiales, dando resultados muy aproximados. Como referencia cabe mencionar que la señal de RF se propaga a mayor distancia cuando esta sale a través de ventana que cuando sale a través de muros y losas, esto debido a que cada material tiene una atenuación distinta y la atenuación presentada por los vidrios es menor a la de los otros materiales como los muros de tabique o lozas de concreto armado. También debe considerarse que los valores obtenidos fueron con los salones vacíos y que estos valores se verán alterados cuando los salones se encuentren completamente llenos de estudiantes.

Como vemos en las pruebas un punto de acceso cubre aproximadamente 3 salones de dirección horizontal en un solo sentido, esto es, el salón donde esta instalado el punto de acceso y los dos salones continuos podría cubrir un salón más en cada sentido pero se prefiere la configuración de tres salones por punto de acceso para mejorar el nivel de la señal y de la conexión hacia el cliente inalámbrico. Por lo que si se quiere cubrir un edifico de 6 salones por nivel, se recomienda utilizar 6 puntos de acceso entre los tres niveles de un edificio con dos canales de frecuencia diferentes.

Con el propósito de distinguir entre puntos de acceso de mayor y de menor cobertura, nombraré puntos de acceso principales a los puntos de acceso que:

Tienen una cobertura mayor

Se encuentran ubicados básicamente en el exterior

Tienen una configuración por lo general de antena omnidireccional o arreglo de antenas.

Tienen antenas para uso en exteriores.

Nombraré puntos de acceso secundarios a los puntos de acceso que:

Tienen una cobertura menor y se encuentran dentro del área de cobertura de un punto de acceso principal.

Se encuentran ubicados básicamente dentro de algún salón o edificio.

Tienen configuración de antenas bidireccionales

Tienen antenas que son instaladas en el techo de un salón.

Haciendo un análisis para cada uno de los salones y los puntos de acceso propuestos dentro de estos, así como basándome en los resultados obtenidos del monitoreo de señal de RF y haciendo las siguientes consideraciones:

1. los salones tienen las mismas dimensiones.

2. utilizan los mismos materiales, todos los muros son del mismo tipo de materia, todos los entrepisos también son del mismo material.

3. están distribuidos de la misma forma en cada uno de los pisos.

4. los puntos de acceso utilizan la misma configuración de antenas y valores de potencia de transmisión.

5. los valores obtenidos en las pruebas son aproximadamente iguales bajo las mismas condiciones (distancias, tipo y cantidad de obstáculos que la señal de RF tiene que cruzar).

Podemos considerar que la atenuación de la señal de RF es igual a la misma distancia y es igual para el mismo numero de muros que tiene que cruzar la señal, ya sea que esta cruce uno en una dirección o en sentido opuesto, esto es en otras palabras, el punto de acceso debe considerarse instalado al centro de un salón, la señal recibida en los salones próximos continuos en ambos extremos, debe ser muy

similar si no es que igual. Por lo tanto, si utilizamos los valores obtenidos de las pruebas y analizamos como se comporta la señal a medida que pasa por los muros y entrepisos, podemos considerar que los valores de recepción dentro de cada salón de un edificio con la configuración de 6 puntos de acceso y 2 canales de frecuencia deben ser como se muestra en la Figura 8.1.3-1.

En el caso de que un edificio se encuentre dentro del área de cobertura de dos puntos de acceso, entonces solo se dispondrá de un canal para hacer la división de celda (cell splitting) dentro de las coberturas de los puntos de acceso principales, por lo que el edificio solo podrá configurarse con 3 puntos de acceso y 1 canal de frecuencia, un punto de acceso por piso pero distribuidos como se muestra en la Figura 8.1.3-1.

La configuración propuesta es así debido a que los puntos de acceso secundarios están dentro de la cobertura de al menos un punto de acceso principal, quedan solo dos canales de RF que pueden ser usados sin interferir al canal del punto de acceso principal. Como se ve en la Figura 8.1.3-1, como máximo se podrá instalar 6 puntos de acceso en un edificio con dos canales de frecuencia, dos puntos de acceso por piso con diferente canal de frecuencia. La configuración dependerá de la disponibilidad de canales.

Al instalarse los equipos como se sugiere y con la configuración de valores de potencia de transmisión, ganancia de antena y patrón de radiación adecuados, se puede evitar interferencia dentro de los edificios entre puntos de acceso que utilicen el mismo canal.

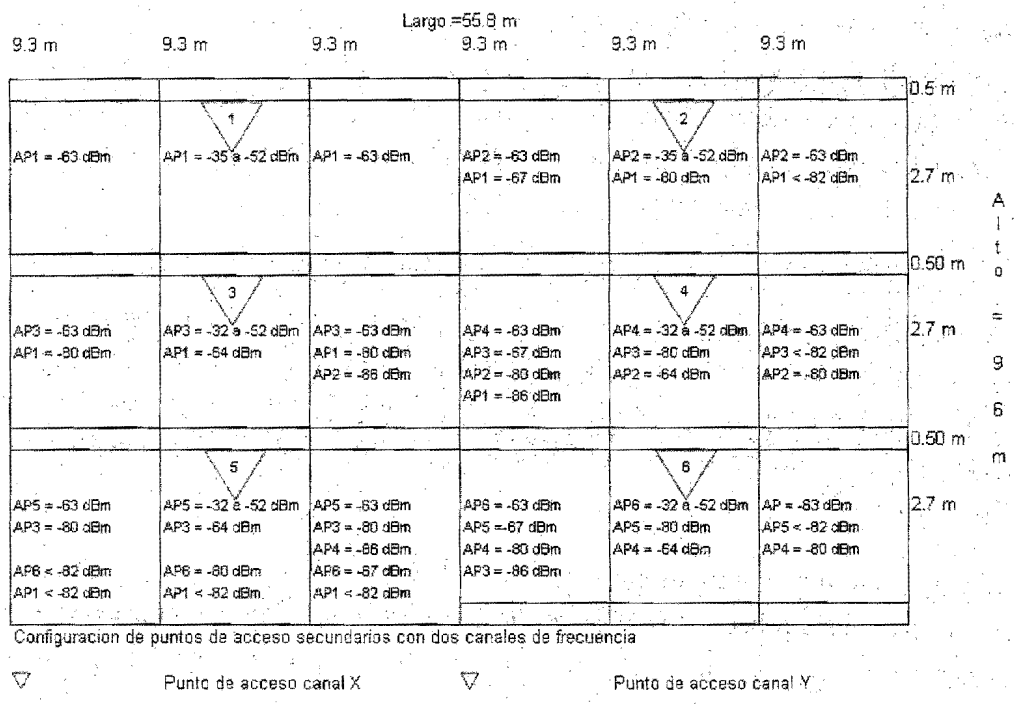


Figura 8.1.3-1 Análisis de datos y configuración de los AP secundarios

Dentro de la etapa de monitoreo de los niveles de señal de la red WLAN se descubrieron 3 Redes inalámbricas con las siguientes características:

SSID	Canal	Velocidad de transmisión Mbps	Encriptación
Comunicaciones	1	11	No
Enepar	11	11	No
ramL3	4	54	No

Tabla 8.1.3-2 Redes inalámbricas detectadas

Si se quiere implementar una red inalámbrica, deben de coordinarse las coberturas y las frecuencias a fin de no interferirse entre ellas. La existencia de redes inalámbricas previas a la propuesta, muestra el interés del sector académico y estudiantil por obtener beneficios que solo las redes inalámbricas pueden ofrecer, rapidez en su implementación, movilidad y costo reducido en comparación con una red por cable. La red inalámbrica debe considerarse en el caso de la escuela como una extensión de la red por cable por lo que no debe pensarse como un sustituto de la red por cable, de hecho la red LAN por cable, se usará como soporte para hacer una ESS, conjunto de servicios extendidos, interconectando cada punto de acceso entre si, al Internet y la intranet. También debe aprovecharse su característica principal que es permitir a los usuarios movilidad.

Se hizo también una prueba de monitoreo para los puntos de acceso principales y los cuales están principalmente ubicados en las explanadas principales de la escuela, a excepción del punto de acceso principal sugerido dentro de la biblioteca.

Las pruebas de monitoreo fueron realizadas en función de la propuesta inicial, y se hicieron de la siguiente manera: se midieron los niveles de Rx entre los puntos de acceso que comparten el mismo canal, el objetivo de esto es determinar si pudiera haber interferencia entre estos puntos de acceso, esto es muy importante debido a que si presentan interferencia muy alta podrían incluso no trabajar o si presentan

interferencia de consideración, reduciría el rendimiento de la red inalámbrica en general. Recuerden que la propagación es distinta en interiores que en exteriores.

La configuración de la propuesta con sus canales es la siguiente:

Punto De acceso principales	Ubicación	Canal
AP1	Entre los edificios A-11, A-7 y A-12	1
AP2	Entre los edificios A-8, A-7, A-6 y A-5	6
AP3	Entre los edificios A-12, A-6, A-1 y edificios de computo	11
AP4	Entre los edificios A-6, A-5, A-4 y A-1	1
AP5	Entre los edificios A-2, A-1, CELE y computo	6
AP6	Entre los edificios A-4, A-3, A-2 y la biblioteca	11
AP7	Entre los edificios A-9, A-3, A-2 y el centro tecnológico	1
AP8	Entre los edificios A-10, A-3, biblioteca y gobierno	6
AP9	dentro de la biblioteca	1
AP10	Entre los edificios A-8, A-5, A-4 y adquicisiones	11

Tabla 8.1.3-3 Ubicación física y asignación de canal a los AP principales

Los valores de la prueba se muestran a continuación:

No	Enlace	Distancia entre puntos de acceso	Canal	resultado
1	AP1-AP4	126 m	1	No hay señal
2	AP1-AP7	240 m	1	No hay señal
3	AP1-AP9	240 m	1	No hay señal
4	AP4-AP7	135 m	1	No hay señal
5	AP4-AP9	120 m	1	No hay señal
6	AP7-AP9	120 m	1	No hay señal
7	AP2-AP5	135 m	6	No hay señal
8	AP2-AP8	210 m	6	No hay señal
9	AP5-AP8	130 m	6	No hay señal
10	AP3-AP6	135 m	11	No hay señal
11	AP3-AP10	126 m	11	No hay señal
12	AP6-AP10	120 m	11	No hay señal

Tabla 8.1.3-4 Resultados del monitoreo en los sitios de los AP principales

El radio de los puntos de acceso, marcado en el gráfico de la propuesta, es de 39 m aproximadamente. Cabe mencionar que el nivel más bajo detectado con nuestro equipo fue de -92 dBm pero no hubo conexión a este nivel. Los valores de prueba fueron Tx = 23 dBm, Gt = 2 dBi, Gr = 2 dBi, por lo que el resultado de "no hay señal" puede ser interpretado como valores mayor a -92 dBm en el sentido negativo.

Por los resultados antes mencionados, podemos estar seguros que no se interferirán los puntos de accesos con la configuración propuesta y esta no se verá modificada, siendo factible este diseño. Sin embargo la configuración de puntos de acceso será distinta, debido a que los equipos que se proponen tienen una potencia de transmisión menor, que es 15 dBm.

Por otro lado y en relación a los sitios de instalación de los puntos de acceso, estos requieren las adecuaciones necesarias para conectar los puntos de acceso con energía eléctrica y conexiones de red como cables ethernet de par trenzado o fibra

óptica. La instalación es muy sencilla y podría hacerse en colaboración con los estudiantes y financiada por la escuela para reducir costos de instalación

Por lo que además recomiendo que se hagan algunas adecuaciones de manera opcional en la distribución de la red eléctrica para brindar a los usuarios de la red inalámbrica, de contactos eléctricos dentro de los edificios y biblioteca, donde los usuarios puedan cargar las baterías de sus computadoras portátiles y/o utilizarlas como fuentes principales de energía.

De acuerdo a los resultados observados durante las pruebas y de acuerdo a la distribución de los edificios propongo la siguiente configuración:

10 puntos de accesos principales distribuidos a lo largo de la escuela 9 en explanadas y 1 dentro de la biblioteca, en función de que no presenta interferencia entre los puntos de acceso con la misma frecuencia, como se muestra en la Figura 8.1.1-1 y como se indica en la Tabla 8.1.3-3. Ubicación física y asignación de canal a los AP principales. Los salones funcionaran también como barrera para evitar que la señal se propague a gran distancia, razón por la cual los puntos de acceso están rodeados en su mayoría por edificios. Si nos referimos a los resultados de las tablas Tabla 8.1.3-1 Resultados del monitoreó dentro de salones y a la Tabla 8.1.3-4 Resultados del monitoreo en los sitios de los AP principales podemos ver que los puntos de acceso principales al menos tienen que pasar un edificio que tiene un muro sólido por un lado y un medio muro con ventana que también atenúan la señal, para poder llegar a otro punto de acceso principal además si vemos en el calculo de la Tabla 8.1.4-1 Calculo de Pr y radio de Fresnel parte 1 a un metro de distancia de la puerta del salón donde se encuentra el punto de acceso de prueba y sumando la distancia hasta el punto de acceso en el interior del salón nos dan aproximadamente 5.5 metros con un muro de tabique de por medio. A esta distancia sin obstáculo nos debe dar en Pr aproximadamente -36 dBm, mientras que lo medido fue de – 58 dBm, por lo tanto tenemos una atenuación debido solo a un muro del edifico de aproximadamente 22 dB, por lo tanto los edificios si funcionan como áreas de confinamiento para los puntos de acceso principales y su cobertura esta

básicamente en las explanadas donde se instalarán. Algunos salones se verán beneficiados por la señal de los puntos de acceso principales debido a que por el lado de las ventanas la señal presenta menor atenuación.

Dentro de cada una de las zonas de cobertura principales se pueden agregar puntos de acceso secundarios ubicados dentro de los salones, con canales de frecuencia distintos a los canales de frecuencia de los puntos de acceso principales de la cobertura donde se encuentren estos, un edificio dentro de la cobertura de un punto de acceso principal podrá disponer de 6 puntos de acceso, haciendo un máximo de puntos de acceso secundarios de 72 entre los 12 edificios de clases y 2 puntos de acceso secundarios en la biblioteca, esto estará condicionado a que todos los salones estén cada uno de ellos, solo dentro de un área de cobertura de un punto de acceso principal. De lo contrario y considerando que los edificios sean cubiertos por 2 puntos de acceso principales, entonces solo se podrá utilizar un canal de frecuencia para los puntos de acceso secundarios y se podrán instalar solo como máximo 3 puntos de acceso secundarios dentro de los edificios Bajo estas condiciones se podrán instalar en total 36 puntos de acceso secundarios dentro de los edificios y uno en la biblioteca., los puntos de acceso secundarios tendrán las siguientes características:

Estarán dentro de un salón para que se limite el nivel de RF que sale hacia fuera del salón y así poder evitar interferencias con otros puntos de acceso

Serán instalados en salones que vayan a ser usados con alta demanda, con la finalidad de optimizar y aprovechar adecuadamente el ancho de banda generado por los puntos de acceso extras, así como el costo de la inversión.

Usarán canales de frecuencia distintas a las frecuencias de los puntos de acceso principales que cubran los edificios donde se van a instalar los puntos de acceso secundarios.

Usaran antenas de menor ganancia, con la finalidad de limitar su alcance, además estas podrán ser antenas direccionales o bidireccionales para enfocar la señal en un área en particular.

La cobertura de los puntos de acceso secundarios de ninguna forma será mayor a la cobertura de los puntos de acceso principales.

Por lo que se podrá instalar como mínimo 10 puntos de acceso principales y 37 puntos de acceso secundarios, 1 de ellos se instalaran en la biblioteca, para hacer un total de 47 puntos de acceso inalámbricos.

Como máximo propuesto se podrá instalar 10 puntos de acceso principales y 74 puntos de acceso secundarios, 2 de los cuales estarán instalados en la biblioteca, para hacer un total de 84 puntos de acceso inalámbricos

8.1.4 Consideraciones de propagación y del estándar 802.11g

Para podernos dar una idea de cual es el alcance de una red inalámbrica y definir valores para la configuración de la red inalámbrica, procedí a realizar el cálculo de un enlace ideal en el espacio libre sin obstáculos.

De la formula de potencia recibida:

$$\Pr = \frac{PtGtGr\lambda^2}{(4\pi * r)^2}$$

Ecuación 8.1.4-1 Potencia recibida

Donde:

Pr = Potencia recibida

Pt = Potencia de transmisión

Gt = Ganancia de la antena de transmisión

Gr = Ganancia de la antena de recepción

r = Distancia entre el punto de transmisión y el recepción

Si despejamos y hacemos la relación Pt/Pr:

$$\frac{Pt}{\Pr} = \frac{(4\pi * r)^2}{GtGr\lambda^2}$$

Esta seria la relación entre la potencia transmitida y la potencia recibida, si ahora aplicamos logaritmo de base 10:

$$10\log\left(\frac{Pt}{\Pr}\right) = 10\log\left(\frac{(4\pi * r)^2}{GtGr\lambda^2}\right)$$

Donde la relación:

$$Po = 10\log\left(\frac{Pt}{\Pr}\right)$$

Es la relación de perdida entre el transmisor y el receptor expresado en logaritmos de base 10, aplicando la ley de la división para los logaritmos al extremo derecho:

$$10\log\left(\frac{Pt}{\Pr}\right) = 10\log(4\pi * r)^2 - 10\log GtGr\lambda^2$$

Aplicando las leyes de los logaritmos para los exponentes y la multiplicación al término de la derecha:

$$10\log\left(\frac{Pt}{\Pr}\right) = 20\log 4\pi + 20\log r - (10\log GtGr + 20\log\lambda)$$

Dado que la longitud de onda λ es función de la velocidad de la luz y de la frecuencia

$$\lambda = \frac{v}{f} \quad \left(\frac{\frac{m}{s}}{\frac{1}{s}}\right)$$

Ecuación 8.1.4-2 longitud de onda

de la señal:

La longitud de onda esta por consiguiente expresada en metros y donde:

$$v = 3*10^8 \ \frac{\mathrm{m}}{s}$$
$$f = 24*10^8 \ \mathrm{Hz}$$

Sustituyendo la formula de la longitud de onda y aplicando la ley de la división para los logaritmos:

$$10\log\left(\frac{Pt}{\Pr}\right) = 20\log 4\pi + 20\log r - (10\log GtGr + (20\log v - 20\log f))$$

Reduciendo y aplicando valores:

$$10\log\left(\frac{Pt}{\Pr}\right) = 21.98 + 20\log r - 10\log GtGr - 169.54 + 187.6$$

Separando por las leyes de la multiplicación a los factores de las ganancias de las antenas:

$$10\log\left(\frac{Pt}{\Pr}\right) = 40.04 + 20\log r - 10\log Gt - 10\log Gr$$

Donde:

$10\log Gt =$ ganancia de la antena del transmisor expresada en dBi
$10\log Gr =$ ganancia de la antena del receptor expresada en dBi

Despejando la potencia de recepción:

$$10\log \Pr = 10\log Pt - 40.04 - 20\log r + 10\log Gt + 10\log Gr$$

Ecuación 8.1.4-3 Potencia de recepción en dBm

Por lo tanta podemos ahora calcular la potencia recibida en un dispositivo WLAN para la red inalámbrica donde la distancia esta expresada en metros con los equipos propuestos. El termino "10 Log Pt" corresponde a la potencia de transmisión del punto de acceso.

Se calcula a su vez el radio de la primera zona de fresnel para darnos una idea de la magnitud del espacio que necesitara esta en su trayecto desde un punto de acceso a otro y ver si se bloque o pasa la señal, la ecuación para el radio de la primera zona de fresnel es:

$$H = \frac{n\lambda d_1 d_2}{d_1 + d_2}$$

donde :

n = la zona de fresnel a determinar

λ = longitud de onda de la señal de RF

d_1 y d_2 = las distancias al punto donde se quiere determinar el radio

Ecuación 8.1.4-4 Radio de la Zona de Fresnel

En la Tabla 8.1.4-1 Resultados de Pr y radio de la zona de Fresnel, se utilizan las formulas para la potencia recibida y el radio de la zona de Fresnel, muestra el alcance de una red inalámbrica sin obstáculos así como la zona de Fresnel a la misma distancia.

Los valores de potencia recibida y transmitida están por lo general expresadas en dBm o mW, se puede cambiar de mW a dBm mediante la siguiente formula:

$$PdBm = 10\log\left(\frac{Pw}{1mW}\right)$$

Ecuación 8.1.4-5 Relación dBm a Watts

Los siguientes son datos del equipo de prueba con el que se hizo las pruebas de campo y los cálculos:

Punto de acceso de Pt = 23 dBm

10logGt = 2 dBi	Ganancia de la ante omnidireccional de punto de acceso
10logGr = 2 dBi	Ganancia de la antena del cliente WLAN

Pr dBm	Pt dBm	Distancia metros	Frecuencia Hz	Gt dBi	Gr dBi	1er Fresnel metros	Zona n	d1 metros	d2 metros
-13.04	23	1	2400000000	2	2	0.18	1	0.5	0.5
-19.06	23	2	2400000000	2	2	0.25	1	1	1
-22.58	23	3	2400000000	2	2	0.31	1	1.5	1.5
-25.08	23	4	2400000000	2	2	0.35	1	2	2
-27.02	23	5	2400000000	2	2	0.40	1	2.5	2.5
-28.60	23	6	2400000000	2	2	0.43	1	3	3
-29.94	23	7	2400000000	2	2	0.47	1	3.5	3.5
-31.10	23	8	2400000000	2	2	0.50	1	4	4
-32.12	23	9	2400000000	2	2	0.53	1	4.5	4.5
-33.04	23	10	2400000000	2	2	0.56	1	5	5
-36.56	23	15	2400000000	2	2	0.68	1	7.5	7.5
-39.06	23	20	2400000000	2	2	0.79	1	10	10
-41.00	23	25	2400000000	2	2	0.88	1	12.5	12.5
-42.58	23	30	2400000000	2	2	0.97	1	15	15
-43.92	23	35	2400000000	2	2	1.05	1	17.5	17.5
-44.86	23	39	2400000000	2	2	1.10	1	19.5	19.5
-45.91	23	44	2400000000	2	2	1.17	1	22	22
-46.84	23	49	2400000000	2	2	1.24	1	24.5	24.5
-47.69	23	54	2400000000	2	2	1.30	1	27	27
-48.46	23	59	2400000000	2	2	1.36	1	29.5	29.5
-49.82	23	69	2400000000	2	2	1.47	1	34.5	34.5
-51.10	23	80	2400000000	2	2	1.58	1	40	40
-52.12	23	90	2400000000	2	2	1.68	1	45	45
-53.04	23	100	2400000000	2	2	1.77	1	50	50
-54.62	23	120	2400000000	2	2	1.94	1	60	60
-55.96	23	140	2400000000	2	2	2.09	1	70	70
-57.12	23	160	2400000000	2	2	2.24	1	80	80
-58.15	23	180	2400000000	2	2	2.37	1	90	90
-59.06	23	200	2400000000	2	2	2.50	1	100	100

Tabla 8.1.4-1 Calculo de Pr y radio de Fresnel parte 1

Pr dBm	Pt dBm	Distancia metros	Frecuencia Hz	Gt dBi	Gr dBi	1er Fresnel metros	Zona n	d1 metros	d2 metros
-59.89	23	220	2400000000	2	2	2.62	1	110	110
-60.64	23	240	2400000000	2	2	2.74	1	120	120
-61.34	23	260	2400000000	2	2	2.85	1	130	130
-61.98	23	280	2400000000	2	2	2.96	1	140	140
-62.58	23	300	2400000000	2	2	3.06	1	150	150
-63.92	23	350	2400000000	2	2	3.31	1	175	175
-65.08	23	400	2400000000	2	2	3.54	1	200	200
-66.10	23	450	2400000000	2	2	3.75	1	225	225
-67.02	23	500	2400000000	2	2	3.95	1	250	250
-67.85	23	550	2400000000	2	2	4.15	1	275	275
-68.60	23	600	2400000000	2	2	4.33	1	300	300
-69.30	23	650	2400000000	2	2	4.51	1	325	325
-69.94	23	700	2400000000	2	2	4.68	1	350	350
-70.54	23	750	2400000000	2	2	4.84	1	375	375
-71.10	23	800	2400000000	2	2	5.00	1	400	400
-71.63	23	850	2400000000	2	2	5.15	1	425	425
-72.59	23	950	2400000000	2	2	5.45	1	475	475
-73.46	23	1050	2400000000	2	2	5.73	1	525	525
-74.25	23	1150	2400000000	2	2	5.99	1	575	575
-74.98	23	1250	2400000000	2	2	6.25	1	625	625
-75.65	23	1350	2400000000	2	2	6.50	1	675	675
-76.27	23	1450	2400000000	2	2	6.73	1	725	725
-76.85	23	1550	2400000000	2	2	6.96	1	775	775
-77.39	23	1650	2400000000	2	2	7.18	1	825	825
-77.90	23	1750	2400000000	2	2	7.40	1	875	875
-78.38	23	1850	2400000000	2	2	7.60	1	925	925
-78.84	23	1950	2400000000	2	2	7.81	1	975	975
-79.28	23	2050	2400000000	2	2	8.00	1	1025	1025
-80.08	23	2250	2400000000	2	2	8.39	1	1125	1125

Tabla 8.1.4-2 Calculo de Pr y radio de Fresnel parte 2

Pr dBm	Pt dBm	Distancia metros	Frecuencia Hz	Gt dBi	Gr dBi	1er Fresnel metros	Zona n	d1 metros	d2 metros
-80.62	23	2450	2400000000	2	2	8.75	1	1225	1225
-81.50	23	2650	2400000000	2	2	9.10	1	1325	1325
-82.14	23	2850	2400000000	2	2	9.44	1	1425	1425
-82.73	23	3050	2400000000	2	2	9.76	1	1525	1525
-83.28	23	3250	2400000000	2	2	10.08	1	1625	1625
-83.80	23	3450	2400000000	2	2	10.38	1	1725	1725
-84.29	23	3650	2400000000	2	2	10.68	1	1825	1825
-84.75	23	3850	2400000000	2	2	10.97	1	1925	1925
-85.19	23	4050	2400000000	2	2	11.25	1	2025	2025
-85.61	23	4250	2400000000	2	2	11.52	1	2125	2125
-86.01	23	4450	2400000000	2	2	11.79	1	2225	2225
-86.39	23	4650	2400000000	2	2	12.05	1	2325	2325
-86.75	23	4850	2400000000	2	2	12.31	1	2425	2425
-87.11	23	5050	2400000000	2	2	12.56	1	2525	2525
-87.44	23	5250	2400000000	2	2	12.81	1	2625	2625
-87.77	23	5450	2400000000	2	2	13.05	1	2725	2725
-88.08	23	5650	2400000000	2	2	13.29	1	2825	2825
-88.38	23	5850	2400000000	2	2	13.52	1	2925	2925
-88.68	23	6050	2400000000	2	2	13.75	1	3025	3025
-88.96	23	6250	2400000000	2	2	13.98	1	3125	3125
-89.23	23	6450	2400000000	2	2	14.20	1	3225	3225
-89.50	23	6650	2400000000	2	2	14.42	1	3325	3325
-89.75	23	6850	2400000000	2	2	14.63	1	3425	3425
-90.00	23	7050	2400000000	2	2	14.84	1	3525	3525
-90.25	23	7250	2400000000	2	2	15.05	1	3625	3625
-90.48	23	7450	2400000000	2	2	15.26	1	3725	3725
-90.71	23	7650	2400000000	2	2	15.46	1	3825	3825
-90.94	23	7850	2400000000	2	2	15.66	1	3925	3925
-91.16	23	8050	2400000000	2	2	15.86	1	4025	4025

Tabla 8.1.4-3 Calculo de Pr y radio de Fresnel parte 3

Pr dBm	Pt dBm	Distancia metros	Frecuencia Hz	Gt dBi	Gr dBi	1er Fresnel metros	Zona n	d1 metros	d2 metros
-91.37	23	8250	2400000000	2	2	16.06	1	4125	4125
-91.58	23	8450	2400000000	2	2	16.25	1	4225	4225
-91.78	23	8650	2400000000	2	2	16.44	1	4325	4325
-91.98	23	8850	2400000000	2	2	16.63	1	4425	4425

8.1.4-4 Calculo de Pr y radio de Fresnel parte 4

Los efectos considerados por la corrección de la curvatura de la tierra para cualquier valor de K debido a la refracción de la señal RF es despreciable a distancias tan cortas como las manejadas en las redes WLAN de corto alcance, por lo que no se considero en el calculo del análisis, también se despreciaron las diferencias de alturas de la antena de transmisión y recepción, debido a que esta va a tener un valor muy pequeño en comparación con los sistemas de repetidor de largo alcance, donde se requiere una altura considerable para cubrir un área muy amplia, además es un sistema punto a multipunto y lo que se requiere es dar cobertura en una área considerable y no a un solo punto. La corrección por la curvatura de la tierra se vuelve despreciable a cortas distancias por lo cual no se aplica en el cálculo.

La altura de la antena se debe fijar con un valor lo más bajo posible para evitar que la señal de los puntos de acceso se propague a grandes distancias.

Por otro lado y en relación a los cálculos obtenidos, Estos nos indica que si no tenemos cuidado de confinar la señal de RF dentro de un espacio cerrado, la señal puede viajar mucho más allá de los limites de la escuela, incluso a una distancia de varios kilómetros, incrementando el riesgo de que un numero mayor de personas maliciosas y ajenas a la escuela tenga acceso a esta. considerando que el nivel más bajo de recepción aceptado por el estándar 802.11g es de -82 dBm, este valor de recepción lo podemos obtener hasta una distancia de 2760 metros siempre y cuando no se encuentran obstáculos entre el transmisor y el receptor, esto es el radio de fresnel de 9.29 metros no debe ser obstruido, para que una señal de RF llegue de un

extremo transmisor a un extremo receptor debe de librar al menos la primera zona de Fresnel, el cálculo del radio de la primera zona de fresnel nos dice que tan sensible es la señal de RF en la banda de 2.4 GHz a los obstáculos, puede verse que a una distancia de 50 metros se requiere que al menos se disponga de 1.25 metros para que pase la primer zona de fresnel. Esto y la reflexión son algunos de los puntos a considerar en la propagación en interiores y por lo cual los valores de Rx no van a ser iguales o cercanos al valor calculado por el método del espacio libre. Si queremos que nuestra señal llegue lo más lejos posible debemos de evitar los obstáculos en la trayectoria de propagación. Debido a la reflexión, refracción, difracción, atenuación debido a los materiales y la perdida en el espacio libre, las distancias que cubre un punto de acceso en interiores se ve reducida si se compara con un punto de acceso que se encuentre en el exterior, en las explanadas.

En el caso de los puntos de acceso que se encuentran en el exterior de los edificios se podría pensar que la propagación esta regida solo por las perdidas en el espacio, pero no es así por que también se puede considerar como propagación en interiores debido a que los puntos de acceso están dentro de áreas cerradas por edificios.

Por otra parte el estándar 802.11g sugiere lo siguiente:

Define 11 canales de frecuencias traslapadas, tres de ellas no son traslapadas, los canales 1, 6 y 11, con un ancho de banda de 22 Mhz totalmente compatible con el estándar 802.11b. (Especificada en la tabla 105 del estándar IEEE 802.11b de 1999, plan de canales de frecuencia), los canales son:

Canal 1 2412 MHz.

Canal 6 2437 MHz.

Canal 11 2462 MHz.

Esto nos indica que si queremos hacer una red amplia y evitar que se interfieran los puntos de acceso, debemos utilizar solo los canales no traslapados, reutilizando los

$$30dBm = Pt + Ga - P_{Cable}$$
$$Ga = 30dBm - Pt + P_{Cable}$$

Ecuación 8.1.4-6 EIRP máximo para 802.11g

canales en otros puntos de acceso. Esto es reutilización de canales de frecuencia comúnmente utilizado en telefonía celular.

La máxima potencia de transmisión (EIRP de acuerdo a la tabla 115 del estándar de la IEEE 802.11b de 1999/Cor. 1-2001, niveles de potencia de transmisión) permitida según la FCC es:

Máxima potencia = 1000 mW

Su equivalente en dBm es: 30 dBm, si hacemos cálculos considerando una potencia de transmisión de 15 dBm y una antena de 15 dBi la suma seria de 30 dBm en el EIRP, esto considerando que no existe perdidas en los cables, pero en verdad si la hay y la perdida dependerá del tipo de cable y de la longitud de este, por lo que la ganancia de la antena no debe ser como máximo el valor que corresponda a la siguiente ecuación:

Donde:

Pt = 15 dBm (Potencia de transmisión del equipo recomendado)

P_{Cable} = 1.1 dB (perdidas en cables y conectores)

Ga = 16.1 dBi (ganancia máximo permitida de antena de transmisión)

Este valor seria el valor máximo permitido de la antena considerando una perdida en los cables de RF de 1.1 dB en todo el tramo.

Para las pruebas realizadas entre puntos de acceso de la misma frecuencia:

Pr= -92 dBm es el nivel mínimo medido, en el cual los puntos de acceso de la misma frecuencia no se interfieren con antenas en los puntos de acceso de 2 dBi en transmisión y recepción. Por lo que si utilizamos la formula de potencia recibida y sustituimos los valores de prueba tenemos:

$$10\log \Pr = 10\log Pt - 40.04 - 20\log r + 10\log Gt + 10\log Gr$$

donde :

$10\log \Pr = -92$ dBm

$10\log Pt = 23$ dBm

$10\log Gt = 2$ dBi

$10\log Gr = 2$ dBi

Sustituyendo valores

-92 dBm $= 23$ dBm $- 40.04 - 20\log r + 2$ dBi $+ 2$ dBi

reduciendo :

-92 dBm $= -13.04 - 20\log r$

Ecuación 8.1.4-7 Nivel de umbral para el equipo de prueba

Ahora si hacemos lo mismo pero con los valores de los equipo que se van a instalar:

$$10\log \Pr = 10\log Pt - 40.04 - 20\log r + 10\log Gt + 10\log Gr$$

donde :

$10\log \Pr = -92dBm$

$10\log Pt = 15dBm$

$10\log Gr = 10\log Gt$

sustituyendo valores

-92 dBm $= 15$ dBm $- 40.04 - 20\log r + 2(10\log Gr)$

-92 dBm $= -25.04 - 20\log r + 2(10\log Gr)$

Ecuación 8.1.4-8 Nivel de umbral para los equipos propuestos

Igualando las dos ecuaciones finales:

$$-13.04 - 20\log r = -25.04 - 20\log r + 2(10\log Gr)$$

reduciendo la expresión :

$$12 = 2(10\log Gr)$$

$$10\log Gr = 6$$

Ecuación 8.1.4-9 Ganancia máxima permitida para los AP principales

Por lo tanto la ganancia de las antenas de los puntos de acceso principales no debe ser mayor a 6 dBi para que los puntos de acceso principales no se interfieran y para que se logren los mismos resultados obtenidos en las pruebas. Aunque debido a que los valores de recepción reales medidos durante la prueba fueron mayores a -92 dBm esto debido a que incluso no fue posible medir este valor, por lo que incluso podemos considerarnos un margen mínimo de diferencia para las antenas propuestas

Por otro lado, debemos utilizar una antena comercialmente disponible con un valor lo más cercano al calculado, encontré una antena omnidireccional que se vende comercialmente en México con un valor muy próxima al valor calculado, la ganancia de la antena propuesta es de 5.2 dBi, incluye el cable de conexión con el conector SMA para conectarse directamente al punto de acceso sugerido.

Por lo tanto la diferencia entre el valor calculado y el valor sugerido de la ganancia de la antena es:

Ganancia de la antena propuesta = 5.2 dBi

Ganancia de la antena calculada = 6 dBi

Diferencia de ganancia = 6-5.2 = 0.8 dB

Tenemos una disminución de 0.8 dB con respecto al calculo, que se puede considerar despreciable, por que, lo que queremos hacer es realmente limitar la

propagación de la señal a larga distancia y su consiguiente interferencia con otros puntos de acceso del presente proyecto, además, debido a que la diferencia entre el valor de recepción esperado (-92 dBm) entre los punto de acceso con la misma frecuencia y el mínimo nivel de recepción del estándar 802.11g es de -82 dBm, da un margen de prácticamente 10 dB, por lo que este diseño esta libre de interferencia entre puntos de acceso principales.

Además que si consideramos que los niveles detectados son en realidad superiores a -92 dBm esto debido a que incluso no fue detectado este valor, sino que simplemente la configuración del equipo de prueba simplemente no detecto la señal y la etiqueta "no hay señal" debe ser interpretada como cualquier valor mayor a -92 dBm en el sentido negativo.

Por lo tanto, considero que la antena propuesta para los puntos de acceso principales esta dentro del valor aceptable por los cálculos.

En casos extremos se pueden insertar un atenuador de un valor que permita disminuir la interferencia con otros puntos de acceso, también pueden ser usados para reducir la cobertura de un punto de acceso.

Entonces Utilizare antenas omnidireccionales de 5.2 dBi para los puntos de acceso principales.

Para nuestra propuesta, también debemos considerar valores de las ganancias de las antenas que nos permitan cubrir solo las regiones de la escuela, esto es, no utilizar antenas de alta ganancia que hagan que la señal cubra incluso área fuera de la escuela, también debe utilizarse el tipo adecuado de antena, direccional, omnidireccional, sectorial o bidireccional. Al ubicar a los puntos de acceso fuera de los salones permitirá cubrir un área mayor que si se ubicaran dentro de los salones y por consiguiente un mayor numero de usuarios, como he sugerido una antena de mayor ganancia a las antenas de prueba, que compensan la baja potencia de transmisión del punto de acceso propuesto.

Por otro lado las antenas omnidireccionales que se proponen tienen un ángulo de radiación en vertical de 27 grados simétricos con respecto a la horizontal, esto es 13.5 grados debajo de la horizontal y 13.5 grados arriba de la horizontal, estos parámetros son los fijados por el fabricante, pero seria conveniente tener antenas con un lóbulo principal más estrecho y orientado hacia el nivel del suelo para poder limitar su propagación a grandes distancias.

Para el calculo de la altura de la antena debemos definir primero un radio de cobertura permitido del punto de acceso, en el caso de los puntos de acceso principales sugerí cubrir las explanadas principales con puntos de acceso que tienen un radio en su cobertura de 39 metros, este radio cubre el área marcada en la Figura 8.1.4-1 Radio de Fresnel.

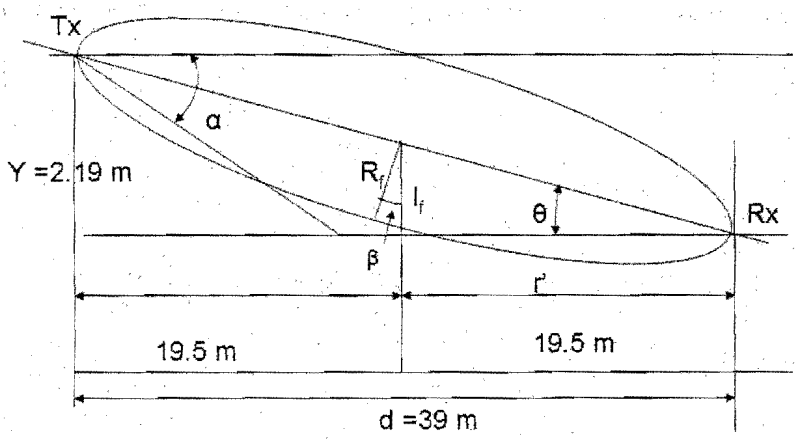


Figura 8.1.4-1 Radio de Fresnel

Ahora si consideramos que a medida que la señal viaja requiere un libramiento de la señal para que el radio de Fresnel no se vea afectado. Veremos una manera de limitar la propagación de la señal de RF es poner las condiciones necesarias para que la zona de Fresnel se empiece a bloquear a partir de cierta distancia.

La zona de Fresnel para cualquier distancia, su radio es mayor cuando se calcula a la mitad de la trayectoria total, también mientras mayor sea la distancia el radio de la zona de Fresnel crecer. Entonces, considerando que se quiere tener un radio de cobertura de 39 m desde el punto de acceso y Considerando que la diferencia de altura es muy pequeña entre el transmisor y receptor como para que el ángulo β. sea significativo, podemos considerar que $R_f = I_f$, donde R_f = 1.1 metros cuando la distancia entre transmisor y receptor es de 39 metros, según los calculo de esta en la Tabla 8.1.4-1 Calculo de Pr y radio de Fresnel parte 1.

Entonces podemos calcular el ángulo de inclinación en el trayecto de la señal del transmisor al receptor.

$$\theta = \tan^{-1}\frac{R_f}{r'}$$

Ecuación 8.1.4-10 Angulo de inclinación del trayecto

Aplicando valores a la formula:

$$\theta = \tan -1\frac{1.1}{19.5}$$
$$\theta = 3.22^{o}$$

Calculando la altura de la antena "y" que representa la altura de la antena del punto de acceso principal:

$$y = d * \tan\theta$$
$$y = 39 * \tan 3.22^{o}$$
$$y = 2.19 \text{ metros}$$

Ecuación 8.1.4-11 Altura de la antena

Por lo que esta será la altura máxima permitida para instalar la antena omnidireccional y que la señal de RF se empiece a bloquear por el piso. El ángulo α representa la mitad del ángulo del lóbulo principal de la antena sugerida en este caso α es de 13.5 grados, por que podemos calcular el lugar adonde llega el borde del lóbulo principal de la ganancia de la antena.

$$d = \frac{y}{\tan\alpha}$$

$$d = \frac{2.19}{\tan 13.5} = 9.12 metros$$

Tabla 8.1.4-5 Distancia de intersección del haz del lóbulo de radiación

Además de que es bloqueada la señal, a partir de aquí la señal llega en línea directa y por reflexión, la recepción será el resultado del la suma de ambas. Obviamente si el receptor de un equipo WLAN es desplazado a una altura mayor este ya no se vera afectado por el bloqueo del radio de Fresnel, pero aquí no podemos hacer más debido a que un intruso, que se encuentre desde afuera de la escuela tratando de recibir la señal de un punto de acceso, puede ubicarse con un equipo que le permita elevar la antena, utilice una antena de mayor ganancia e incluso utilice un amplificador bidireccional para poder recibir la señal de cualquier punto de acceso inalámbrico o simplemente entrar a la escuela y hacerse pasar como estudiante.

Obviamente a menor altura de la antena, menor distancia de cobertura también y mayor seguridad pero si realmente no queremos que nadie "toque" la señal de RF de los puntos de acceso, entonces simplemente no hay que utilizar esta tecnología.

Pero no hay problema la verdadera seguridad de las redes inalámbricas corre a cargo de protocolos de autenticación y de encriptación, más si queremos un sistema realmente protegido debemos utilizar el conjunto de todas las técnicas que nos brinden seguridad desde todos los puntos de vista.

Las antenas para los puntos de acceso secundarios ubicados dentro de los salones se determinan de la siguiente manera:

Las pruebas reportadas y las consideraciones fueron obtenidas con una configuración de salida de potencia (EIRP) de 25 dBm (Pt = 23 dBm y Ga = 2 dBi).

Por lo tanto la configuración del punto de acceso recomendado con su antena no debe rebasar este valor para evitar que los puntos de acceso secundarios se interfieran.

La potencia de transmisión del punto de acceso propuesto es de 15 dBm.

$$25dBm \geq 15dBm + Ga - Pcable$$
$$25 - 15 + 0.1 \geq Ga$$
$$10.1 \geq Ga$$

Ecuación 8.1.4-12 Ganancia de Gr máxima

Por lo tanto la ganancia de la antena propuesta no debe ser mayor a 10.1 dBi para obtener los mismos resultados de propagación obtenidos en las pruebas, si además consideramos que el último salón tiene una recepción de -63 dBm y el valor mínimo permitido para la comunicación en redes 802.11g es de -82 dBm, por lo que con una antena de 10 dBi tenemos un margen de recepción de:

Margen de recepción = 82-63 = 19 dB

Esto significa que aun disminuyendo la ganancia de la antena en un margen ligeramente menor a 19 dB, todavía tendremos un valor de recepción aceptable para los salones de los extremos y por lo tanto obtendremos la cobertura deseada.

Si usamos antenas bidireccionales comercialmente disponibles de Ga = 4 dBi, la diferencia de ganancias se vera reflejada proporcionalmente en el nivel de recepción de los salones de los extremos, La diferencia es de:

Diferencia de ganancias de antenas = 10 -4 = 6 dB

Por lo que también el margen de recepción disminuirá en la misma proporción:

Disminución del margen de recepción = 19 – 6 = 13 dB

Por lo que aun usando antenas bidireccionales de 4 dBi debemos tener un nivel de potencia de recepción adecuado para comunicarnos con el punto de acceso secundario hasta una distancia no mayor a un salón hacia los lados, con un margen de 13 dB antes de que la recepción de la señal se vea afectada. Además esta antena tiene un patrón de radiación que nos ayudara a evitar interferencia con los puntos de acceso inferiores o superiores, debido a que la ganancia en estas direcciones es menor a 0 dBi.

Se utilizo el valor de 4 dBi debido a que comercialmente esta disponible en el mercado y reúne las características necesarias para ser usadas dentro de los salones son de montaje en el techo y son bidireccionales. Es una antena bidireccional de 4 dBi en direcciones opuestas (0 y 180 grados) y de 0 dBi en sentido transversal (90 y 270 grados).

Los requerimientos de rendimiento para el estándar 802.11g se definen en la tabla 91 del estándar 802.11a-1999 de la IEEE, requerimiento de rendimiento de la recepción, es el siguiente:

Velocidad de transmisión Mbps	Sensibilidad mínima dBm
6	-82
9	-81
12	-79
18	-77
24	-74
36	-70
48	-66
54	-65

Tabla 8.1.4-6 Requerimiento de rendimiento para el receptor 802.11g

Esto nos indica que la velocidad de transmisión dependerá de la señal recibida y esta en función de las perdidas por el espacio libre, por reflexión y obstáculos por lo que mientras menos obstáculos estén en la trayectoria de punto de acceso hacia un cliente WLAN mejor será la señal y por consiguiente mayor el rendimiento de la red WLAN. El valor mínimo aceptable para una comunicación en el estándar 802.11g esta definido a -82 dBm, por lo que cualquier valor inferior a este debe considerarse como no aptos para la comunicación en la red WLAN propuesta.

8.1.5 Equipo WLAN propuesto para los puntos de acceso

En base a los resultados obtenidos, se propone el siguiente equipo para los puntos de acceso principales con antenas omnidireccionales:

Equipo	Modelo	Marca	Observaciones
Antena Omnidireccional	MAO24005PTMSMA	Maxrad	ganancia de 5.2 dBi
Punto de acceso 802.11g	TEW-410APBPplus	Trendnet	Tx = 15 dBm

Tabla 8.1.5-1 Equipo para los puntos de acceso principales

El equipo propuesto para los puntos de accesos secundarios y que serán instalados básicamente dentro de los salones es el siguiente:

Equipo	Modelo	Marca	Observaciones
Antena Bidireccional	MHA2400PTMSMA	Maxrad	Incluye cable 4 dBi
Punto de acceso 802.11g	TEW-410APBPplus	Trendnet	Tx = 15 dBm

Tabla 8.1.5-2 Equipo para los puntos de acceso secundarios

8.1.6 Equipo LAN propuesto para la interconexión

Para poder conectar los puntos de acceso entre ellos y hacia la conexión de Internet, se requiere hardware de red que permita la comunicación entre los distintos puntos de acceso, la configuración propuesta es a través de 4 VLAN´s que permitirán:

Contener el tráfico como resultado del confinamiento de los broadcast de dominio de red.

Reduce la necesidad de desplegar costosos ruteadores dentro de la red para contener el tráfico, reducen el costo debido a que los switchs son relativamente más baratos que una ruteador.

Permiten mayor flexibilidad de diseño si los comparamos con una red con ruteadores. Debido a que mediante configuración dentro de los switchs, se puede configurar la red por completo. Las VLAN´s propuesta pueden ser segmentadas en VLAN´s más pequeñas, mientras que el diseño de los ruteadores es estático y requiere más equipo para su modificación.

Por otro lado existen básicamente tres tipos de switch:

Switch no administrables

Los switchs no administrables son dispositivos de capa 2 del modelo OSI y como su nombre dice no se requiere configurar ningún parámetro para su operación. Actualmente todos los hubs están siendo remplazados por los switch que permiten optimizar el desempeño de la red.

Switchs de capa 2 administrables.

Los switch de capa 2 son dispositivos de capa 2 del modelo OSI y requieren configuración para poder crear VLAN´s, además de tener las funciones de los switch no administrables.

Switch de capa 2 y 3

Los switch de capa 2 y 3 del modelo de referencia OSI, tienen todas las ventajas de los dos anteriores pero además tienen la ventaja de que pueden rutear tráfico entre las VLAN´s y hacia el gateway, este es el equipo principal que utilizare para la infraestructura de la red inalámbrica.

Son tres los pasos básicos indispensables para la configuración son:

1. configurar las 4 la VLAN´s dentro del switch.
2. configurar la propagación de las VLAN´s a otros switchs
3. rutear las VLAN´s

La configuración de las VLAN´s significa que se tienen que agrupar los puertos que van a configurar a las VLAN´s, en nuestro caso son 4 VLAN´s que se tienen que hacer para agrupar los puntos de acceso en sus respectivas VLAN´s.

La propagación de las VLAN´s permitirá hacer que el tráfico de una VLAN en un switch pase a otra switch que tiene la misma VLAN, sobre un enlace simple de Ethernet y nos permitirá extender cualquier VLAN en particular sobre toda la red. Esto es, se puede tener una VLAN definida con hosts en diferentes switchs.

El ruteo permitirá rutear el tráfico de cualquier VLAN a cualquiera de las otras VLAN´s e incluso hacia la salida de Internet. Por lo que la operación de la red desde el punto de vista de los usuarios será muy similar a estar operando dentro de una red segmentada por ruteadores. La configuración es transparente para los usuarios y estos no se ven afectados por el diseño de la red. Pudiendo incluso incrementar o disminuir el numero de VLAN´s dentro de la red según sea necesario.

El equipo recomendado para la LAN y que implementará la ESS, es el siguiente:

EQUIPO LAN

Equipo	Modelo	Marca	Cantidad	Observaciones
Switch catalyst	WS-3550-24-EMI	Cisco	4	24 puertos 10/100 Mbps 2 interfaces GBIC
Switch catalyst	WS-3550-12G	Cisco	1	10 interfaces GBIC, 2 puertos 10/100/1000BaseT
Interfaces GBIC 1000Base-SX	WS-G5484	Cisco	8	Para fibra multimodo hasta 550 m
Firewall	PIX501-UL-BUN-K9	Cisco	1	
ADSL router	827-4V	Cisco	1	

Tabla 8.1.6-1 Equipo propuesto para soportar la ESS

El proyecto se contempla realizar por fases u opciones, lo que permitirá realizar inversiones parciales en tres etapas o fases:

Fase 1 instalación de 10 puntos de acceso principales

Fase 2 instalación de 24 puntos de acceso secundarios, 2 puntos de acceso secundarios para 6 salones de de cada edificio (A-1 al A-12), más 2 puntos de acceso secundarios de la biblioteca

Fase 3 instalación de hasta 48 puntos de acceso secundarios en los dos niveles restantes de cada edificio (A-1 al A-12).

Por otro lado y regresando a la configuración de las VLAN´s estas que tendrán la siguiente configuración para los puntos de acceso principales:

No	VLAN	PUNTOS DE ACCESO PRINCIPALES	PUERTOS ETHERNET	FASE
1	VLAN1	AP1	1	1
2	VLAN1	AP3	1	1
3	VLAN2	AP2	1	1
4	VLAN2	AP4	1	1
5	VLAN2	AP10	1	1
6	VLAN3	AP5	1	1
7	VLAN3	AP6	1	1
8	VLAN3	AP7	1	1
9	VLAN4	AP8	1	1
10	VLAN4	AP9	1	1

Tabla 8.1.6-2 Configuración de los AP principales en las VLAN´s

Sumando un total de 10 puertos Ethernet requeridos para su conexión.

Para los puntos de acceso secundarios, primero defino un nombre para cada uno, en función del edificio donde se encuentran instalados y el nivel donde están, por último un número 1 o 2 puesto que es el número de puntos de acceso máximos que pueden instalarse en cada nivel de un edificio, por ejemplo:

Punto de acceso A0111

Los tres primeros caracteres indicaran el numero de edificio, en este caso se refiere al edificio A-1, el cuarto carácter indicara el nivel, en este caso 1 indica el nivel 1 o planta baja, por ultimo el quinto carácter indicara un de los dos posibles puntos de acceso de ese nivel.

Por lo tanto la configuración para los puntos de acceso secundarios fase 2 dentro de las VLAN´s es el siguiente:

No	VLAN	PUNTOS DE ACCESO SECUNDARIOS EN EDIFICIOS	PUERTOS ETHERNET	FASE
1	VLAN1	A1111-A1112	2	2
2	VLAN1	A1211-A1212	2	2
3	VLAN2	A0511-A0512	2	2
4	VLAN2	A0611-A0612	2	2
5	VLAN2	A0711-A0712	2	2
6	VLAN2	A0811-A0812	2	2
7	VLAN3	A0111-A0112	2	2
8	VLAN3	A0211-A0212	2	2
9	VLAN3	A0311-A0312	2	2
10	VLAN3	A0411-A0412	2	2
11	VLAN4	A0911-A0912	2	2
12	VLAN4	A1011-A1012	2	2
13	VLAN4	BIB11-BIB12	2	2

Tabla 8.1.6-3 Configuración de los AP secundarios en las VLAN´s fase 2

Requiriendo 26 puertos ethernet para su conexión.

La configuración para los puntos de acceso fase 3 es de la siguiente manera:

No	VLAN	PUNTOS DE ACCESO SECUNDARIOS EN EDIFICIOS	PUERTOS ETHERNET	FASE
1	VLAN1	A1121-A1122	2	3
2	VLAN1	A1131-A1132	2	3
3	VLAN1	A1221-A1222	2	3
4	VLAN1	A1231-A1322	2	3
5	VLAN2	A0521-A0522	2	3
6	VLAN2	A0531-A0532	2	3
7	VLAN2	A0621-A0622	2	3
8	VLAN2	A0631-A0632	2	3
9	VLAN2	A0721-A0722	2	3
10	VLAN2	A0731-A0732	2	3
11	VLAN2	A0821-A0822	2	3
12	VLAN2	A0831-A0832	2	3
13	VLAN3	A0121-A0122	2	3
14	VLAN3	A0131-A0132	2	3
15	VLAN3	A0221-A0222	2	3
16	VLAN3	A0231-A0232	2	3
17	VLAN3	A0321-A0322	2	3
18	VLAN3	A0331-A0332	2	3
19	VLAN3	A0421-A0422	2	3
20	VLAN3	A0431-A0432	2	3
21	VLAN4	A0921-A0922	2	3
22	VLAN4	A0931-A0932	2	3
23	VLAN4	A1021-A1022	2	3
24	VLAN4	A1031-A1032	2	3

Tabla 8.1.6-4 Configuración de los AP secundarios en las VLAN´s fase 3

Requiriendo un total 48 puertos ethernet para su conexión. Sumando todos los puertos ethernet requeridos para el proyecto (fase 1, 2 y 3) en total son 84 puertos ethernet solo para conectar los puntos de acceso inalámbricos.

Se instalará 1 switch de 24 puertos por cada VLAN, por consiguiente necesitamos 4 switchs con capacidad de ruteo entre VLAN en la parte de acceso. Además de que estos switch irán conectados a través de enlaces de fibra óptica hacia un switch principal que llamaremos de distribución, concentrara a las VLAN´s para después pasarlos al ruteador y/o firewall de salida y después al MODEM ADSL.

Los protocolos encargados de rutear entre las VLAN para estos switchs son:

Inter-switch link o IEEE 802.10

Los switchs propuesto son de capa 2 y 3 del modelo OSI, por lo que tiene capacidad de ruteo.

Todas estas tecnologías están basadas en mecanismos de multiplexión de la capa 2 del modelo OSI:

8.1.7 Interconexión de la red inalámbrica

La interconexión de la red inalámbrica tiene como finalidad intercomunicar los puntos de acceso entre si, esto es se creara una red de conjunto de servicios extendidos ESS con servicio de Internet. Los puntos de acceso se conectan a su respectivo switch mediante cable UTP categoría 5, mientras que el up link de los switchs de acceso utilizan fibra óptica multi-modo al switch de distribución.

La interconexión es como se muestra en la siguiente figura.

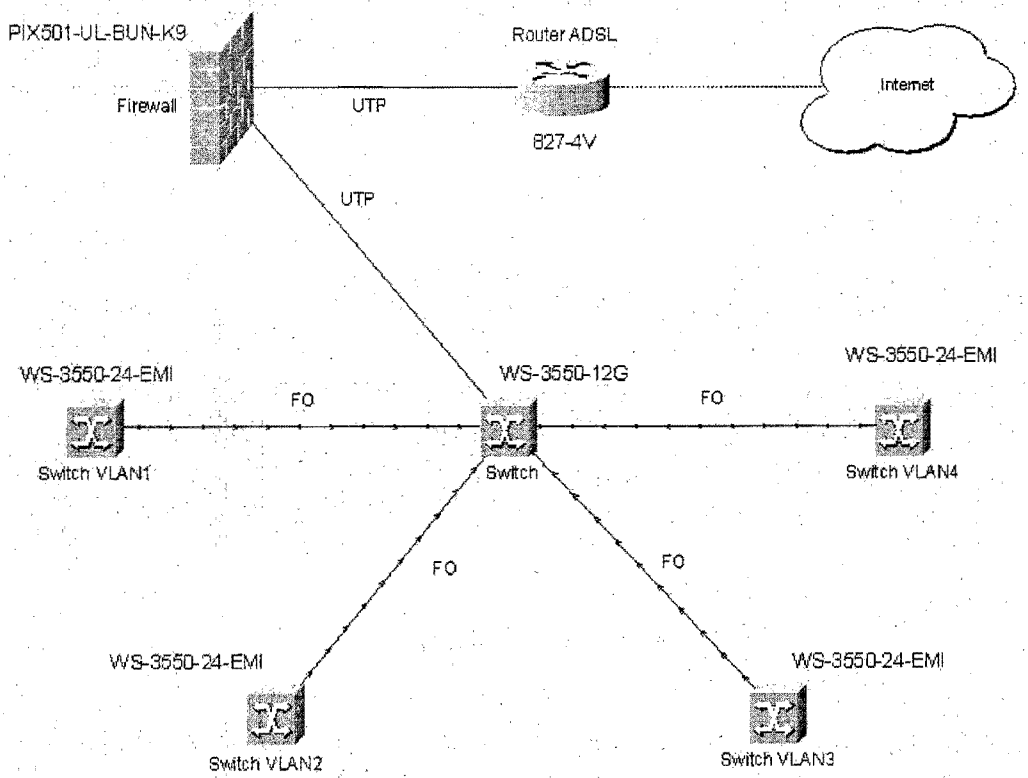


Figura 8.1.7-1 Red LAN propuesta para soportar la ESS

Se hicieron sub redes de clase B para albergar a las de 256 usuarios por VLAN. Además de requiere de 4 VLAN por lo que si hacemos subneting en la clase B debo tomar tres bits del hostid para hacer el subneting, por lo tanto la máscara de red será 255.255.224.0 (19 bits).

Se crearan las siguientes subredes:

SUBREDES VLAN´S

VLAN	Subred	Hosts	Broadcast
VLAN1	172.21.32.0	172.21.32.1 - 172.21.63.254	172.21.63.255
VLAN2	172.21.64.0	172.21.64.1 - 172.21.95.254	172.21.95.255
VLAN3	172.21.96.0	172.21.96.1 - 172.21.127.254	172.21.127.255
VLAN4	172.21.128.0	172.21.128.1 to 172.21.159.254	172.21.159.255

Tabla 8.1.7-1 VLAN´s de la red

Por lo tanto tenemos un máximo de 2^{13}-2 direcciones de red por VLAN, 8190 direcciones IP para los clientes inalámbricos y puntos de acceso, suficientes para configurar puntos de acceso y clientes.

La configuración de IP de la red es el siguiente:

ASIGNACIÓN DE DIRECCIONES EN VLAN1

DISPOSITIVO	IP	MÁSCARA	OBSERVACION
INTERFÁZ VLAN1	172.21.32.1	255.255.224.0	PUERTO DE LA VLAN
RESERVADO	172.21.32.2-172.21.32.10	255.255.224.0	APLICACIONES FUTURAS
$AP_{PRINCIPALES}$	172.21.32.11-172.21.32.12	255.255.224.0	AP1 Y AP3
$AP_{SECUNDARIOS2}$	172.21.32.13-172.21.32.16	255.255.224.0	FASE 2
$AP_{SECUNDARIOS3}$	172.21.32.17-172.21.32.24	255.255.224.0	FASE 3
CLIENTES WLAN	172.21.32.25-172.21.63.254	255.255.224.0	POR DHCP

Tabla 8.1.7-2 Configuración VLAN1

ASIGNACIÓN DE DIRECCIONES EN VLAN2

DISPOSITIVO	IP	MÁSCARA	OBSERVACIÓN
INTERFÁZ VLAN2	172.21.64.1	255.255.224.0	PUERTO DE LA VLAN
RESERVADO	172.21.64.2-172.21.64.10	255.255.224.0	APLICACIONES FUTURAS
$AP_{PRINCIPALES}$	172.21.64.11-172.21.64.13	255.255.224.0	AP2, AP4 Y AP10
$AP_{SECUNDARIOS2}$	172.21.64.14-172.21.64.21	255.255.224.0	FASE 2
$AP_{SECUNDARIOS3}$	172.21.64.22-172.21.64.37	255.255.224.0	FASE 3
CLIENTES WLAN	172.21.64.38-172.21.95.254	255.255.224.0	POR DHCP

Tabla 8.1.7-3 Configuración VLAN2

ASIGNACIÓN DE DIRECCIONES EN VLAN3

DISPOSITIVO	IP	MÁSCARA	OBSERVACIÓN
INTERFÁZ VLAN3	172.21.96.1	255.255.224.0	PUERTO DE LA VLAN
RESERVADO	172.21.96.2-172.21.96.10	255.255.224.0	APLICACIONES FUTURAS
$AP_{PRINCIPALES}$	172.21.96.11-172.21.96.13	255.255.224.0	AP5, AP6 Y AP7
$AP_{SECUNDARIOS2}$	172.21.96.14-172.21.96.21	255.255.224.0	FASE 2
$AP_{SECUNDARIOS3}$	172.21.96.22-172.21.96.37	255.255.224.0	FASE 3
CLIENTES WLAN	172.21.96.38-172.21.127.254	255.255.224.0	POR DHCP

Tabla 8.1.7-4 Configuración VLAN3

ASIGNACIÓN DE DIRECCIONES EN VLAN4

DISPOSITIVO	IP	MÁSCARA	OBSERVACIÓN
INTERFÁZ VLAN4	172.21.128.1	255.255.224.0	PUERTO DE LA VLAN
RESERVADO	172.21.128.2-172.21.128.10	255.255.224.0	APLICACIONES FUTURAS
$AP_{PRINCIPALES}$	172.21.128.11-172.21.128.12	255.255.224.0	AP8 Y AP9
$AP_{SECUNDARIOS2}$	172.21.128.13-172.21.128.18	255.255.224.0	FASE 2
$AP_{SECUNDARIOS3}$	172.21.128.19-172.21.128.26	255.255.224.0	FASE 3
CLIENTES WLAN	172.21.128.27-172.21.159.254	255.255.224.0	POR DHCP

Tabla 8.1.7-5 Configuración VLAN4

Los puntos de acceso principales irán instalados en el exterior en postes o soportes que sujeten a los gabinetes que protegerán al equipo activo. Los puntos de acceso secundarios se deberán instalar al centro del salón propuesto, fijados en el techo del mismo, los puntos de acceso podrán ser instalados en gabinetes, pero las antenas al igual que el anterior caso deberán estar adecuadamente descubiertas para que las ondas electromagnéticas puedan salir hacia las zonas de cobertura.

También requerimos dos subredes para el firewall y el router ADSL por lo que en clase C, hacemos subneting tomando los dos bits más significativos del hostid, por lo tanto la máscara de red es 255.255.255.224 (27 bits). Con 3 bits para el subneting tenemos hasta 2^3-2 =6. Se crearon las siguientes subredes:

SUBREDES LAN´S

LAN	Subred	Hosts	Broadcast
1	192.168.32.0	192.168.32.1 - 192.168.63.254	192.168.63.255
2	192.168.64.0	192.168.64.1 - 192.168.95.254	192.168.64.255

Tabla 8.1.7-6 Sub redes LAN

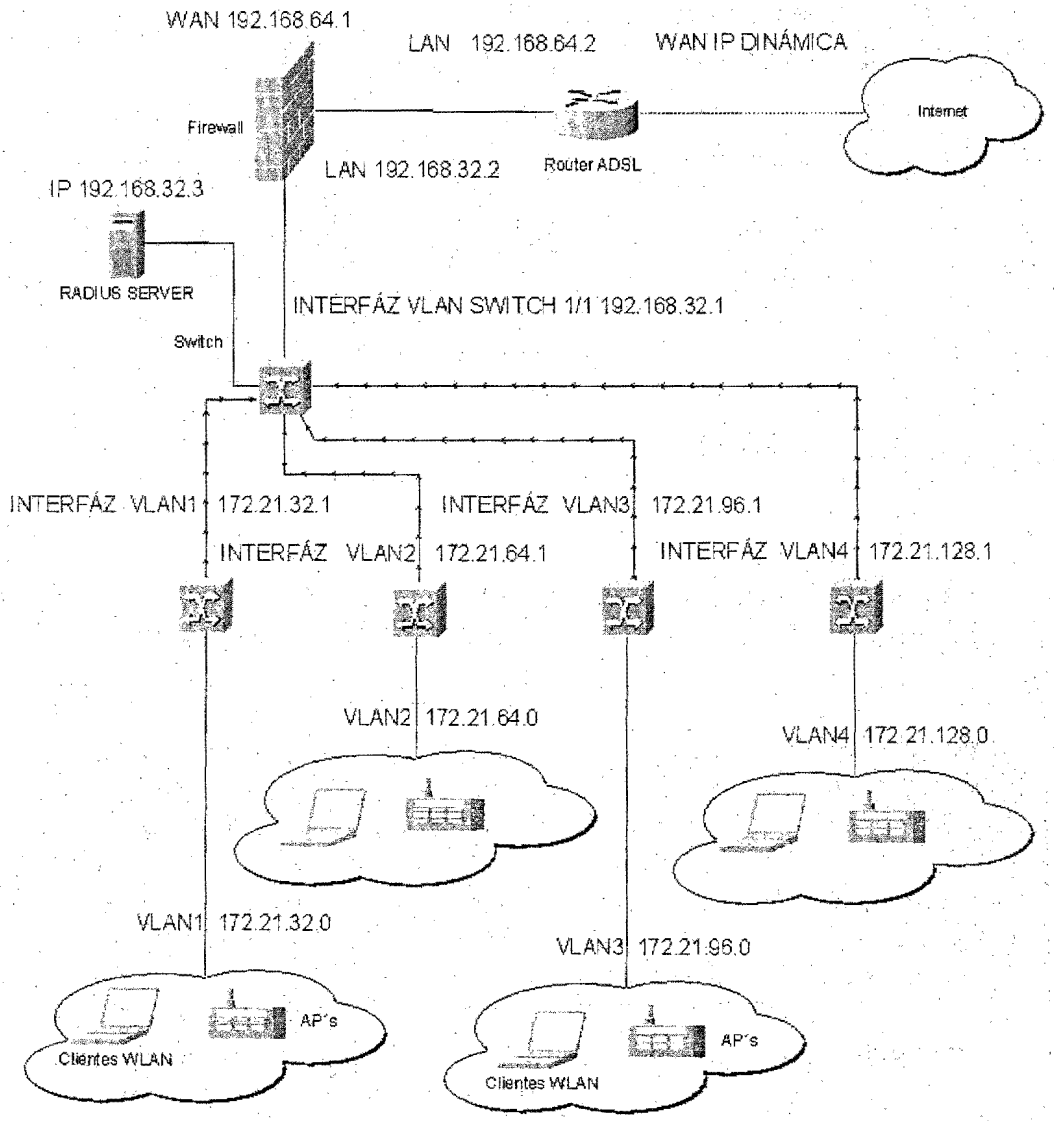
La configuración del resto de la red es el siguiente:

ASIGNACIÓN DE DIRECCIONES LAN

DISPOSITIVO	IP	MÁSCARA	OBSERVACIÓN
INTERFAZ SWITCH1/1	192.168.32.1	255.255.255.224	PUERTO DE SALIDA
FIREWALL ENTRADA	192.168.32.2	255.255.255.224	HACIA LA RED LAN
SERVIDOR RADIUS	192.168.32.3	255.255.255.224	PARA LA RED WLAN
OTROS SERVIDORES	192.168.32.4 – 192.168.63.254	255.255.255.224	WEB, FTP, DNS, ETC.
FIREWALL SALIDA	192.168.64.1	255.255.255.224	HACIA LA WAN
ADSL ROUTER	192.168.64.2	255.255.255.224	LAN
ADSL ROUTER	IP DINAMICA		DIRECCIÓN WAN DINAMICA ASIGNADA POR EL PROVEEDOR

Tabla 8.1.7-7 Configuración en redes LAN

Se muestra a continuación el diagrama de la red inalámbrica.



La ubicación de las VLAN´s dentro de la ENEP Aragón es la siguiente:

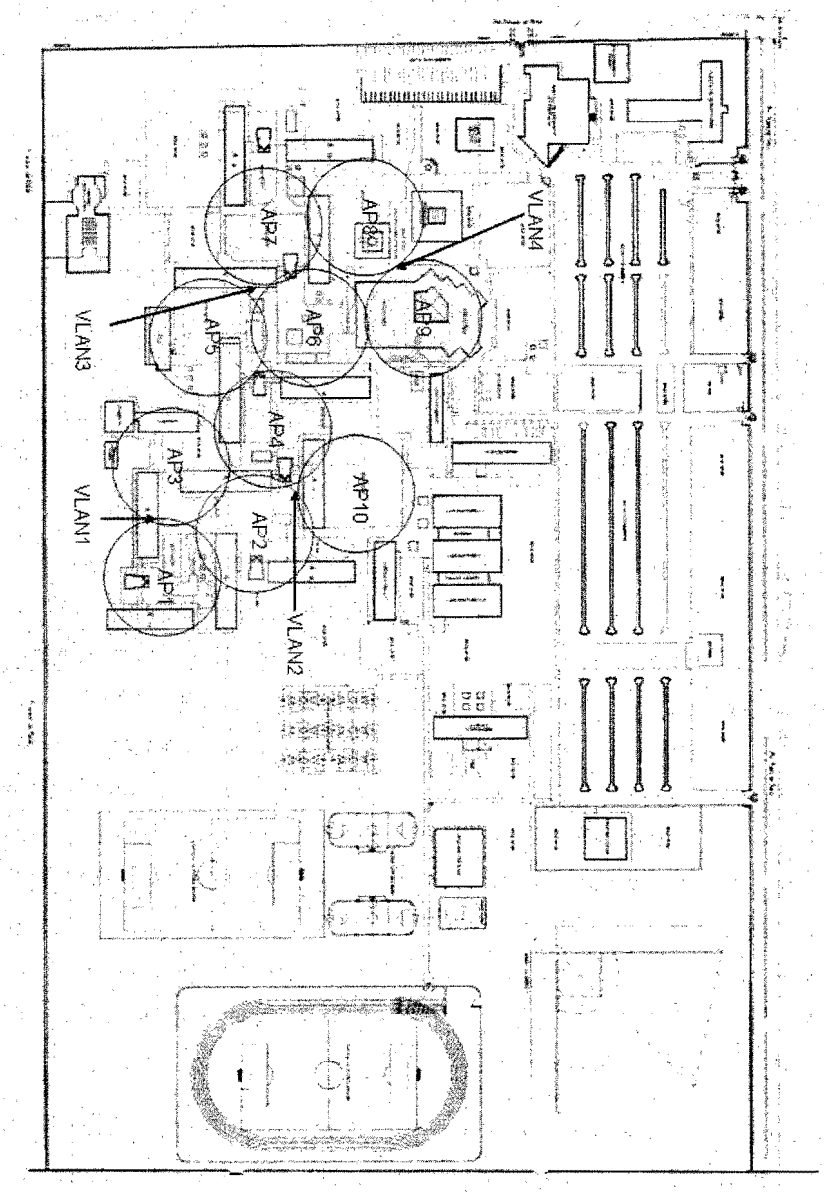


Figura 8.1.7-4 Ubicación de las VLAN´s

8.1.8 Interconexión a Internet

Para proporcionar conexión a Internet la red inalámbrica existen actualmente de manera comercial tres opciones:

Tecnología	Proveedor	Velocidad de transmisión	Costo
MODEM ADSL	TELMEX	254 Kbps a 2.048 Mbps	$349 a $4599
MODEM SATELITAL	DIRECWAY	128 Kbps a 2.048 Mbps	$977.5 a $20849
MODEM POR CABLE	CABLEVISION	64 Kbps a 512 Kbps	$90 a $453

Tabla 8.1.8-1 Opciones de conexión a Internet

Se recomienda el uso de la conexión con MODEM ADSL debido a su costo y a su disponibilidad así como a su mejor relación costo beneficio y mayor margen de crecimiento. Esta es ofrecida por la compañía de TELMEX. El único requisito para esta es disponer de una línea telefónica sobre la cual viajar la señal del ADSL, con la posibilidad de utilizar el teléfono normal (POTS) y el acceso a Internet simultáneamente, se puede solicitar el servicio en varios anchos de banda pero se sugiere utilizar el ancho de banda de 512 Kbps como mínimo y escalar a medida que se requiera mejorar el servicio y/o se incremente la demanda del servicio. Si el máximo soportado por un ADSL no bastara para ofrecer el servicio se pueden contratar más de un servicio para atender a la red inalámbrica. Obviamente esto implica hacer cambios en la parte WAN, para poder tener dos salidas WAN hacia Internet o unas salida al Internet y otra a la intranet.

La línea telefónica previamente contratada con el servicio de prodigy infinitum es pasada a través de un divisor (splitter) de voz y datos con entrada RJ-11 y dos salidas RJ-11: una es para conectar directamente un teléfono convencional y por la cual solo sale señal de voz, la siguiente es una salida para datos por la cual solo

pasa la señal del ADSL, esta salida se conecta mediante un cable con conectores RJ-11 hacia el MODEM ADSL para líneas POTS. El MODEM tiene como interfaces una conexión RJ-11 para la conexión ADSL, una conexión RJ-45 para la conexión Ethernet de 10/100 Mbps en el extremo de la LAN.

La conexión del MODEM ADSL es como se muestra en la figura siguiente:

La configuración se establece con valores definidos por el proveedor de servicio, este debe proveer de los siguientes parámetros:

VPi virtual path ID (identificador de la ruta virtual)

VCi virtual channel ID (identificador del canal virtual)

Estos dos parámetros están expresados en valores numéricos enteros positivos y corresponden a la configuración típica de ATM.

Existen las opciones de configuración para la calidad del servicio y también dependen del plan contratado:

UBR tasa de transferencia de bits no disponible

VBR tasa de transferencia de bits varia, en tiempo real y en no tiempo real

CBR tasa de transferencia de bits constante

Estos parámetros definen la calidad del servicio solicitada u ofrecida por el proveedor y también son definidos por el proveedor.

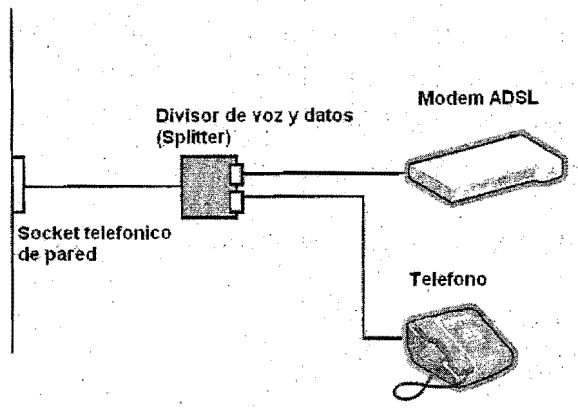


Figura 8.1.8-1 Conexión del ADSL

En esta configuración el MODEM ADSL no incluye las funciones de ruteador, este será instalado de forma separada, permitiendo más versatilidad y confiabilidad de los equipos.

8.1.9 Recomendaciones para el equipo de los clientes inalámbricos

Los usuarios que quieran hacer uso de los servicios de la red inalámbrica deberán contar con los siguientes requisitos técnicos:

Computadora portátil de 1.5 GHz mínimo

Sistema operativo Windows XP con las actualizaciones para compatibilidad con redes inalámbricas y WPA Windows XP KB826942-x86-ESN.exe y Q815485_WXP_SP2_x86_ENU.exe o el service pack 2 de Windows

Software Antivirus	Norton antivirus (recomendado)
Software Firewall	Norton Internet security (recomendado)
Tarjeta de red	PCMCIA o USB con el estándar 802.11g y su software de instalación. Verificar que cumpla con el estándar (802.11g aprobado)

y que no sea un borrador de este (802.11g draft) que este certificada por el organismo Wi-Fi. Se recomienda tarjetas de red que tengan soporte para el protocolo de encriptación AES basado en hardware.

8.1.10 Cobertura de la red inalámbrica

El alcance de la red inalámbrica puede recalcularse nuevamente para hacer correcciones del alcance de esta, ahora con el total de los puntos de acceso, la cobertura propuesta es una estimación teórica pero es muy cercana a la real creada con los puntos de acceso ya instalados, pero puede medirse nuevamente con un kit de monitoreo una vez que la red este completamente instalada para determinar el alcance real. Los valores de prueba inicial cumplen varios objetivos:

Determinar el alcance aproximado de la red inalámbrica

Determinar el tamaño y posición de los puntos de acceso

Determinar como reutilizar los canales de frecuencia

Determinar posibles interferencias entre puntos de acceso

Descubrir puntos de acceso existentes que deben ser integrados o eliminados según sea la necesidad.

Aún cuando se puede implementar seguridad desde el momento en que se proponen las coberturas, en este caso no es posible por que la escuela es un espacio publico donde entra y sale mucha gente, por lo que si alguien quiere atacar a la red inalámbrica puede hacerlo sin que tenga que recibir señal de RF de algún punto de acceso desde afuera de los limites de la escuela. Simplemente tiene que pasar como estudiante para estar dentro de la escuela y tener a su alcance el nivel de RF de la red inalámbrica que le permitan monitorear los paquetes de datos de esta. es por eso que la seguridad realmente corre a cargo de los protocolos de encriptación y de autenticación del protocolo WPA, que por el momento no ha sido

rota a nivel internacional, además de que antes de que termine el año 2004 se tendrá disponible el estándar de seguridad WPA2 que se es considerado como la seguridad más robusta para redes inalámbricas y la cual puede ser implementada en la red propuesta cuando se tenga el estándar definitivo y existan en el mercado las actualizaciones de software y Firmware requeridos para su implementación. Comercialmente conocido como WPA2 pero definido como el estándar de la IEEE, 802.11i es la más nueva propuesta de seguridad para redes WLAN.

8.1.11 Seguridad en la red inalámbrica

La seguridad de la red inalámbrica debe implementarse en los clientes inalámbricos, los puntos de acceso y la red de soporte para el conjunto de servicios extendidos (ESS):

La seguridad de los usuarios será implementada básicamente mediante software como son: un sistema operativo sin huecos de seguridad, esto es deben instalarse todos los parches que eviten riesgos de seguridad con el equipo, así como un sistema antivirus para detectar virus informáticos y un firewall para bloquear contenido no deseado, programas que se conectan de manera automática a Internet, redes no autorizadas, protocolos, puertos, que permita la detección de intrusiones y el bloqueo de correo spam.

La seguridad a través de los puntos de acceso se implementa primero diseñando la red inalámbrica de manera que la cobertura no viaje largas distancias (control de la zona de radiación) y esté al alcance de personas mal intencionadas, lamentablemente la escuela es un sitio público por lo que cualquier persona puede entrar al área de cobertura de los puntos de acceso inalámbricos, después habilitando el nivel de encriptación más robusto permitido por el punto de acceso. En el caso de los propuestos, estos disponen del nivel más alto de encriptación publica conocida, el cual es el AES (estándar de encriptación avanzada), a su vez realiza autenticación del usuario mediante un servidor RADIUS. Por el momento la propuesta es usar TKIP en la encriptación.

El estándar de seguridad AES estará implementado en el protocolo de seguridad WPA2, como ya se mencionó AES es el más avanzado método de encriptación de uso público disponible WPA2 podrá estar disponible según la alianza de empresas Wi-Fi totalmente aprobado a fines del año 2004. AES es soportado por el punto de acceso propuesto. Por lo que será totalmente compatible con WPA2.

La seguridad desde la red está implementada en base a que para empezar la red inalámbrica no está conectada a la red local (DMZ), por lo que no puede ingresar a los equipos como servidores que operan aplicaciones de misión crítica, mediante un servidor de RADIUS (servicios de autenticación de usuarios de marcación de acceso remoto), el cual tiene una base de datos donde se tiene registrados a todos los usuarios validos de la red, este servidor radius, realizara la autenticación de los usuarios utilizando el protocolo de autenticación extensible protegido PEAP, el cual asegura el proceso de autenticación, también desde la red se implementan políticas de administración y de usuarios que refuerzan la seguridad al implantar mecanismos para identificar, controlar y supervisar a los usuarios suscriptos a la red.

La autenticación corre por cuenta de un servidor RADIUS para los usuarios dentro de la red inalámbrica. Este puede ser montado en Linux con un software también de licencia libre llamado Freeradius o se puede utilizar Windows Server 2003 con su aplicación llamada IAS (Internet access Server) el cual soporta RADIUS.

Con la instalación de un firewall puede incrementarse la seguridad a su vez que permite mediante los bloqueos de tráfico de direcciones IP, direcciones MAC, puertos TCP y UDP, protocolos de capas de aplicación como FTP, TFTP, DNS, SMTP, ETC, podrá optimizarse y aprovecharse adecuadamente el acceso a Internet. También permitirá que la conexión a Internet solo sea utilizada por las aplicaciones adecuadas sin que se haga un mal uso del ancho de banda de la red inalámbrica. Opcionalmente los puntos de acceso podrán bloquear cada uno un máximo de 40 direcciones MAC. La seguridad se vera reforzada además por las políticas de administración y de usuario.

8.1.12 Funciones de la administración

La escuela definirá un o unos administradores los cuales administraran el uso de la red inalámbrica.

Los administradores darán mantenimiento a la red inalámbrica (puntos de acceso, el cableado eléctrico y cableado UTP o fibra óptica, switches, router MODEM ADSL y el servidor RADIUS), así como a todo el equipo de red asociado a la red inalámbrica.

Realizarán trámites necesarios para el control de las cuentas de usuarios de la red inalámbrica, supervisaran periódicamente el estado de las instalaciones de la red inalámbrica, puntos de acceso, antenas, cableado de alimentación, cableado de red y UTP o de fibra óptica.

Realizarán monitoreos periódicos que le permitan determinar si existen intrusiones maliciosas a la red.

Configurarán los equipos para aumentar la seguridad y el rendimiento de esta.

Administraran el sistema, dando de alta o bloqueando direcciones IP, MAC, puertos, páginas y protocolos no deseables y que afecten el rendimiento y seguridad de la red.

Realizaran reportes del desempeño de la red que permitan evaluar la conveniencia de incrementar el ancho de banda para el Internet, así como implementar nuevas funciones dentro de esta.

Podrán solicitar a los usuarios la información que este requiera para comprobar que son usuarios validos dentro de la red.

8.1.13 Políticas de usuarios

Las políticas de usuarios nos ayudaran a mantener orden y control sobre los usuarios de red inalámbrica y pueden ser divididas en tres partes:

1. Políticas de acceso

2. Políticas de utilización de la red

3. Políticas de seguridad

Las políticas de acceso que propongo son las siguientes:

Para accesar a la red, los usuarios primero deberán cubrir los requisitos que la escuela defina como necesarios para identificar plenamente a los futuros usuarios.

Deberán pagar una cuota definida por la escuela y la cual debe ser utilizada para el financiamiento de la red inalámbrica.

Los usuarios deberán renovar su cuenta cada semestre, por lo que implica que solo habrá cuentas con duración de un semestre.

Se cancelara el acceso a la red inalámbrica a toda persona que rompa las medidas de seguridad así como toda persona que haga un mal uso de la red.

El acceso a la red será con equipos que sean aprobados por los administradores y que sean compatibles con el estándar 802.11g. La red se configuró solo para esta y no admite dispositivos o configuraciones para 802.11b.

Se restringirá indefinidamente el acceso a cualquier persona que atente contra los equipos inalámbricos y por cable que forman parte de la red inalámbrica.

Los usuarios de la red inalámbrica tendrán acceso solo si son miembros de la comunidad universitaria: alumno, maestros, administrativos, ex alumnos y trabajadores de la ENEP Aragón.

Las políticas para el uso de la red propuestas son las siguientes:

La red debe ser utilizada como un medio para obtener información relativa a cualquiera de las materias que se imparten de manera oficial dentro de la escuela

Queda prohibido el acceso a páginas de contenido obsceno, con contenido sexual

El uso de la red para hacer transacciones de compra o venta queda bajo responsabilidad del usuario. La administración y las autoridades de la escuela quedan libres de responsabilidad en la pérdida, intercepción y modificación de información confidencial del usuario.

Esta prohibido el uso de mensajes obscenos, ya sean estos audio, video o texto con los programas de mensajeria electrónica.

Será sancionado severamente a toda persona que se detecte enviando aplicaciones con virus para computadoras.

Se sancionará el envió de correo spam.

Se sancionara severamente a toda persona que intente saturar de tráfico indeseable, a la red inalámbrica.

Las políticas de seguridad son las siguientes:

Los usuarios serán responsables de la actualización de sistema operativo y demás software, se deberá contar con las actualizaciones del sistema operativo sobre todo aquellas concernientes a la seguridad y la conectividad de redes inalámbricas.

Los usuarios deben utilizar solo las tarjetas de red inalámbrica cuyas direcciones MAC están registradas con el administrador de red.

Las direcciones MAC no registradas serán bloqueadas en el sistema. Se fijarán multas o sanciones por el uso de tarjetas con MAC no registradas.

Para poder cambiar de tarjeta de red inalámbrica, Los usuarios están obligados a reportar la dirección MAC de una nueva tarjeta que hayan adquirido para ser utilizada dentro de la red inalámbrica de la escuela. La dirección MAC anterior será dada de baja del sistema.

Solo podrá ser utilizada una dirección MAC por cuenta

El uso de los equipos WLAN solo deberá ser en el modo de infraestructura y no en el modo ad-hoc.

No podrán prestar sus cuentas a otros usuarios, las cuentas son únicas de cada usuario. Esto también implica que no se podrá intercambiar direcciones MAC (tarjetas de red inalámbricas) y cuentas de usurarios (nombre de usuario y clave)

La administración se reserva el derecho de bloquear todo el tráfico que considere afecte el rendimiento y seguridad de la red.

Es obligación y responsabilidad de usuario mantener a su equipo libre de virus, por lo cual este debe contar con un antivirus permanentemente actualizado.

La seguridad en los equipos de los usuarios corre a cargo de los usuarios, por lo que estos deben de contar con software antivirus y firewall, así como darle un buen uso a su equipo.

Los usuarios podrán hacer transacciones comerciales por Internet, como compras de libros, disco, etc. Pero la seguridad de su información y de la transacción corre por cuenta del mismo usuario.

Los usuarios deberán mostrar su credencial de usuario de red WLAN cuando las autoridades competentes así lo requieran.

De no ser usuarios validos serán reportados a las autoridades competentes dentro de la escuela siendo acreedores a la sanción que esta autoridad considere.

Como miembros de la red inalámbrica deberán proporcionar información que ayude a descubrir a posibles intrusos, así como informar de posibles huecos en la seguridad de la red.

Los usuarios y no usuarios de la red, miembros de la escuela o personal ajeno a esta serán severamente sancionados y puestos a disposición de las autoridades competentes, si se les descubre dañando el equipo de red inalámbrico, como puntos de acceso, cableado, antenas, conectores y todo aquel componente que degrade o perjudique el desempeño de la red inalámbrica.

8.1.14 Análisis de costos.

El proyecto de la red inalámbrica puede dividirse en dos fases:

La fase inicial será la instalación de los puntos de acceso principales que se propone instalar en las explanadas, fuera de los salones además de instalar la red LAN que servirá de infraestructura para soportar la ESS (conjunto de servicios extendidos. Esto permitirá cubrir explanadas y pasillos principales de la escuela.

La segunda fase será la instalación de 2 puntos de acceso secundarios dentro de cada edificio de clases de la escuela, lo cual permitirá dar servicio a por lo menos 6 salones de cada uno de los edificios de clases. Dando servicio de Internet e intranet a todas las carreras que se imparten en la escuela.

La tercera fase es cubrir todos los salones de clases de la escuela, considerando un promedio de 6 salones por nivel de cada edificio dando un total de 72 salones aproximadamente.

Dado el tamaño de la infraestructura posterior a esto se puede crecer la red inalámbrica agregándole servidores de:

Correo electrónico, web, FTP, DNS, DCHP, etc.

Lo cual permitirá tener una intranet inalámbrica que después se puede interconectar a la intranet existente. La idea de poner servidores es con la intención de que cada carrera tenga una página web donde publiquen información relacionada con su carrera como son:

Eventos culturales

Noticias

Calendarios de fechas importantes

Recomendaciones

Investigaciones y proyectos

Por su parte se pueden crear servidores de FTP y de correo para poder compartir información, documentos, fotos, diagramas, críticas, etc.

Se realizó una cotización del equipo básico requerido para el proyecto con la intención de mostrar el costo real del proyecto. La cotización se realizo en base a costos unitarios y no por volumen con diferentes proveedores. Las cifras en todos los casos, están en pesos Mexicanos a octubre del 2004. Para la primera fase, el costo del proyecto es el siguiente:

Primera fase WLAN

No	Equipo	Modelo	Marca	Costo unitario	Cantidad	Unidad	Subtotal
1	Antena omnidireccional	MDO24005PTMSMA	Maxrad	$2,000.00	10	Pzas	$20,000.00
2	Punto de acceso	TEW-410APBplus	Trendnet	$2,150.00	10	Pzas	$21,500.00
3	Gabinete metálico	SYG-058NM	SYSCOM	$932.00	10	Pzas	$9,320.00
4	Poste 2.2 m	Calabaza	Laiting	$2,072.50	10	Pzas	$20,725.00
5	Cable UTP Categoria 5	1583A	Belden	$3.00	1000	metros	$3,000.00
6	Conector RJ-45	5-558530	AMP	$3.00	20	Pzas	$60.00
	SUBTOTAL						$74,605.00
	IVA						$11,190.75
	TOTAL						$85,795.75

Tabla 8.1.14-1 Primera fase WLAN

Para la red LAN se realizaron dos cotizaciones, una con equipo Cisco y otra con equipo 3com, esto debido a la diferencia de precios entre ambas, mi propuesta es la opción con equipo Cisco, tiene más prestaciones, rendimiento y calidad.

Primera fase LAN Cisco

No	Equipo	Modelo	Marca	Costo unitario	Cantidad	Unidad	Subtotal
1	Switch acceso	WS-C3550-24-SMI	Cisco	$27,236.80	4	Pzas	$108,947.20
2	Switch de distribución	WS-C3550-12G	Cisco	$90,898.52	1	Pzas	$90,898.52
3	Modulo GBIC	WS-G5484	Cisco	$4,547.20	8	Pzas	$36,377.60
4	Firewall	PIX-501-UL-BUN-K9	Cisco	$9,048.00	1	Pzas	$9,048.00
5	Router MODEM ADSL	CISCO827-4V	Cisco	$9,085.35	1	Pzas	$9,085.35
6	Fibra óptica multi-modo	MLD6002	Belden	$24.50	1600	metros	$39,200.00
7	Conectores SC	FSCMMBL	Panduit	$98.00	4	Pzas	$392.00
8	Conectores SC	FSCMMRD	Panduit	$98.00	4	Pzas	$392.00
9 10	servidor Windows 2003 (RADIUS, DHCP, ETC)		HP	$20,000.00	1	Pzas	$20,000.00

SUBTOTAL	$314,340.67
IVA	$47,151.10
TOTAL	$361,491.77

Tabla 8.1.14-2 Primera fase LAN Cisco

Primera fase LAN 3com

No	Equipo	Modelo	Marca	Costo unitario	Cantidad	Unidad	Subtotal
1	Switch de acceso 3226	3CR17500-91	3com	$6,472.17	4	Pzas	$25,888.68
2	Switch de distribución 4050	3C17708	3com	$118,114.00	1	Pzas	$118,114.00
3	1000BASE SX GBIC	3CGBIC91	3com	$4,313.27	4	Pzas	$17,253.08
4	1000BASE SX SFP	3CSFP91	3com	$3,966.92	4	Pzas	$15,867.68
5	Superstack Firewall	3CR16110-95-US	3com	34720.83	1	Pzas	34720.83
6	Router MODEM ADSL 3030	3C13630	3com	7061.15	1	Pzas	7061.15
7	Fibra óptica multi-modo	MLD6002	Belden	$24.50	1600	metros	$39,200.00
8	Conectores SC	FSCMMBL	Panduit	$98.00	4	Pzas	$392.00
9	Conectores LC	1588706-1	AMP	130	4	Pzas	520

SUBTOTAL	$259,017.42
IVA	$38,852.61
TOTAL	$297,870.03

Tabla 8.1.14-3 Primera fase LAN 3com

Se puede elegir entre la versión con equipo Cisco o la versión con equipo 3com, los costos totales de cada una de estas es el siguiente:

No	VERSION DE LA PRIMERA FASE	COSTO
1	COSTO DE LA PRIMERA FASE CON EQUIPO CISCO	$447,287.52
2	COSTO DE LA PRIMERA FASE CON EQUIPO 3COM	$383,665.78

Tabla 8.1.14-4 Costos totales según la versión

El costo de la segunda fase es el siguiente:

Segunda fase WLAN

No	Equipo	Modelo	Marca	Costo unitario	Cantidad	Unidad	Subtotal
1	Antena Bi-direccional	MHA2400PT	Maxrad	$1,000.00	26	Pzas	$26,000.00
2	Punto de acceso	TEW-410APBplus	Trendnet	$2,100.00	26	Pzas	$54,600.00
3	Gabinete	SYG-075	Syscom	$1,099.00	26	Pzas	$28,574.00
4	Cable UTP Categoría 5	1583A	Belden	$3.00	2600	Metros	$7,800.00
5	Conectores RJ-45	5-558530	AMP	$3.00	52	Pzas	$156.00

Subtotal	$117,130.00
IVA	$17,569.50
TOTAL	$134,699.50

Tabla 8.1.14-5 Segunda fase WLAN

Para la tercera y última fase el costo es el siguiente:

Tercera fase WLAN

No	Equipo	Modelo	Marca	Costo unitario	Cantidad	Unidad	Subtotal
1	Antena Bi-direccional	MHA2400PT	Maxrad	$1,000.00	48	Pzas	$48,000.00
2	Punto de acceso	TEW-410APBplus	Trendnet	$2,100.00	48	Pzas	$100,800.00
3	Gabinete	SYG-075	Syscom	$1,099.00	48	Pzas	$52,752.00
4	Cable UTP Categoría 5 metros	1583A	Belden	$3.00	2600	Metros	$7,800.00
5	Conectores RJ-45	5-558530	AMP	$3.00	52		$156.00

Subtotal	$209,508.00
IVA	$31,426.20
TOTAL	$240,934.20

Tabla 8.1.14-6 Tercera fase WLAN

El costo total del proyecto que incluye la suma de las tres fases es el siguiente:

No	Proyecto final	Costo
1	WLAN con LAN Cisco	$822,921.22
2	WLAN con LAN 3com	$759,299.48

Tabla 8.1.14-7 Costo total del proyecto

Por otra parte regresando al estándar 802.11 (edición de 1999), este define dentro del frame de la MAC el AID (identificador de asociación) que es utilizado para el poleo de ahorro de energía y define un máximo de 2007 equipos asociados a un punto de acceso, esto no debe entenderse como equipos transmitiendo

simultáneamente. Solo significa que el punto de acceso es capaz de reconocer un máximo de 2007 equipos WLAN que en cualquier momento estén dispuestos a transmitir durante el periodo de contención por el medio utilizando CSMA/CA. El número de equipos que estén transmitiendo simultáneamente dependerá de la velocidad de conexión a la que logren conectarse cada uno de los dispositivos, al tráfico existente en cada punto y la relación señal a ruido del enlace individual de cada cliente WLAN con su respectivo punto de acceso. Algunos fabricantes recomiendan un máximo de hasta 256 usuarios por punto de acceso. Por lo que si multiplicamos este valor por el número de puntos de acceso de la primera fase tendremos un total de 2560 usuarios, para la suma de la primera fase y segunda fase, el número de usuarios en la red inalámbrica llegaría a 9216 usuarios y así de la misma manera con la tercera fase.

El objeto de una red inalámbrica es proveer de acceso inalámbrico en áreas donde una red por cable no llega, además de soportar la movilidad de los clientes inalámbricos, esta es su principal ventaja sobre la red por cable. Además de que permitirá que los alumnos conecten su propios equipos a la red inalámbrica.

Conclusiones

De acuerdo a investigaciones dentro de otras universidades, dentro y fuera de México, vemos que las redes inalámbricas están siendo ampliamente utilizadas dentro de campus universitarios, por lo que concluyo que en un corto tiempo la ENEP Aragón se verá en la necesidad de seguirle el paso a las universidades que ya disponen de una red inalámbrica. El estudio realizado en el presente trabajo demuestra como es posible implementar una red inalámbrica en las instalaciones de la ENEP Aragón. Los estudios y mediciones prácticas realizadas indican en conclusión que dicha red es técnicamente viable.

Las actuales tecnologías de las redes inalámbricas son el logro de avances muy importantes en el área de al computación y las radiocomunicaciones, más sin embargo, el avance que van a tener estas tecnologías inalámbricas en los próximos años no se detendrá aquí, para empezar están por aprobarse estándares que permitirán incrementar la velocidad (802.11n), incremento en el nivel de seguridad (802.11i) y opciones para la calidad de servicio (802.11e), así como redes inalámbricas de área amplia WiMax (802.16), permitirán que estas tecnologías se hagan de uso masivo no solo en campus universitarios, también en sectores industriales y comerciales, requiriendo personal capacitado para diseñar, implementar, administrar y reparar el equipo asociado a estas redes, por lo que será de gran importancia que se considere su estudio dentro de algún plan de estudio de ingeniería, debe considerarse que actualmente existen programas de certificación para las tecnologías wireless como son: CWNA y CWSP (Certified Wireless Network Administrador y Certified Wireless Security Professional respectivamente) que respaldan el conocimiento del personal que toma estas certificaciones con reconocimiento a nivel internacional y como están basadas en estándares son independientes de la marca de cualquier producto. Estas certificaciones demuestran el interés de los diferentes sectores a nivel internacional y la confianza que tienen en el desarrollo de las redes WLAN.

Por el dado del la implementación y de acuerdo al análisis realizado, donde se hacen sugerencias basadas en los estándares de la familia 802.11 y cálculos matemáticas para determinar valores de las ganancias de las antenas, podemos concluir que la red inalámbrica puede instalarse en la ENEP Aragón, siempre y cuando siga la configuración propuesta ya sea en su totalidad o solo algunas de las fases.

El estándar actual 802.11g y WPA tienen un considerable nivel de avance en cuanto a seguridad se refiere, permitiendo esto, implementar una red inalámbrica con las medidas de seguridad necesarias para su operación dentro de un campus universitario como la ENEP Aragón, donde el numero de usuarios puede ser considerablemente alto, permitiendo autenticar de manera independiente y única a cada uno de sus usuarios, manteniendo un adecuado nivel de tráfico con un nivel de seguridad aceptable. Para fines de este año esta por aprobarse el estándar 802.11i (WPA2), que puede mejorar enormemente la seguridad dentro de la red inalámbrica propuesta. El equipo sugerido para la implementación soporta la encriptación AES (estándar de encriptación avanzada), por lo que concluyo además, que esta red inalámbrica no solo es completamente segura sino que puede ser actualizada al nuevo estándar en cuanto este sea liberado y se encuentre disponible el firmware para la actualización.

El financiamiento de la red, suena exagerado pero si se considera que se puede recurrir al apoyo del sector estudiantil, solicitar apoyo a la industria y mediante recursos de la propia escuela, concluyo que si se puede y debe instalarse una red inalámbrica en la ENEP Aragón, para beneficio de las actuales y próximas generaciones de estudiantes a licenciatura e ingeniería dentro de este honorable centro de estudios.

Las redes inalámbricas encontradas durante el estudio demuestran una vez más el interés y necesidad por implementar una red inalámbrica, no solo para pequeños grupos sino para todo aquel que muestre enteres por obtener beneficios de las redes WLAN.

Apéndice

$$V = \frac{1}{\sqrt{\mu_0 \kappa_0}} = 299795637.7 \frac{m}{s}$$

$$K_0 = 8.854 \times 10^{-12} \frac{Faradays}{metro}$$

$$\mu_0 = \frac{4\pi}{10} \times 10^{-6} \frac{Henries}{metro}$$

Ecuación 1 Velocidad de la luz

$$VWSR = \frac{1 + \sqrt{\frac{Potenciareflejada}{Potenciadirecta}}}{1 - \sqrt{\frac{Potenciareflejada}{Potenciadirecta}}}$$

Ecuación 2 Corrección de la altura por la curvatura de la tierra

$$h_k = \frac{d_1 \times d_2}{2Kr}$$

$$r = 6378000 metros$$

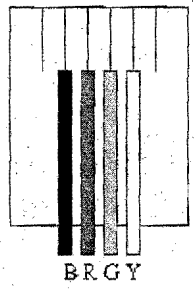
Ecuación 3 VWSR

Nombre	Significado	Frecuencia	Longitud de onda
VLF	Very low frecuency	3-30 KHz.	100-10 Km.
LF	Low frecuency	30-300 KHz.	10-1 Km.
MF	Medium frecuency	300-3000 KHz.	1-0.1 Km.
HF	High frecuency	3-30 MHz.	100-10 m.
VHF	Very high frecuency	30-300 MHz.	10-1 m.
UHF	Ultra high frecuency	300-3000 MHz.	1-0.1 m.
SHF	Super high frecuency	3-30 GHz.	10-1 cm.
EHF	Extremely high frecuency	30-300 GHz.	10-1 mm.

Tabla 1 Clasificación de las señales de RF

Tipo de clima	valor de K
Zona polar	6/5 a 4/3
Zona templada	4/3
Zona calida	4/3 a 3/2

Tabla 2 Valores del factor K



Primer par: rojo y verde
segundo par: negro y amarillo

Figura 1 Configuración de RJ-11

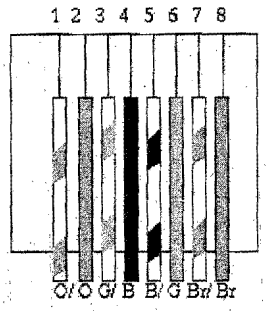


Figura 2 Configuración de RJ-45

Código de color para T-568B

Pin	Color	Par	Nombre
1	white/orange	2	TxData +
2	orange	2	TxData -
3	white/green	3	RecvData +
4	blue	1	
5	white/blue	1	
6	green	3	RecvData -
7	white/brown	4	
8	brown	4	

Tabla 3 Configuración de pins de RJ-45

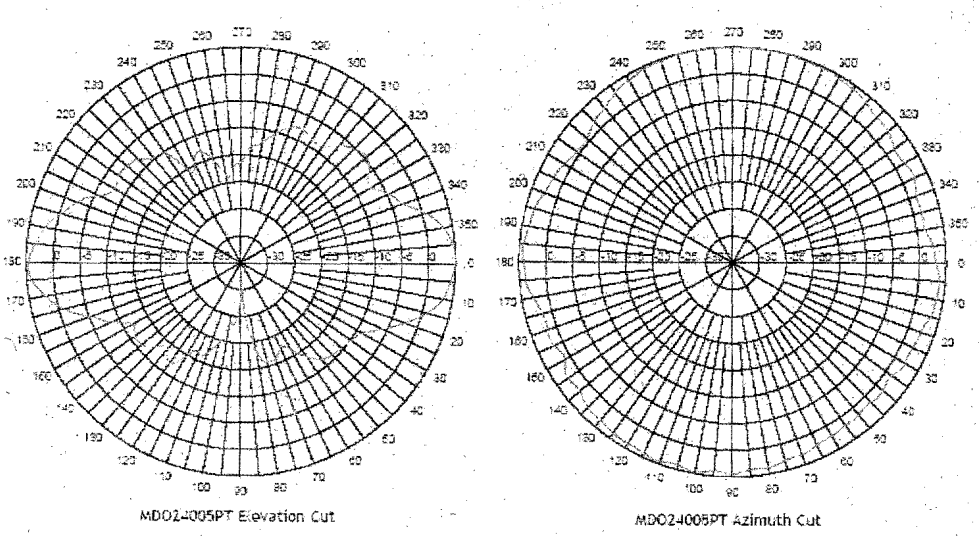


Figura 3 Patrón de radiación de la antena MDO24005PTMSMA

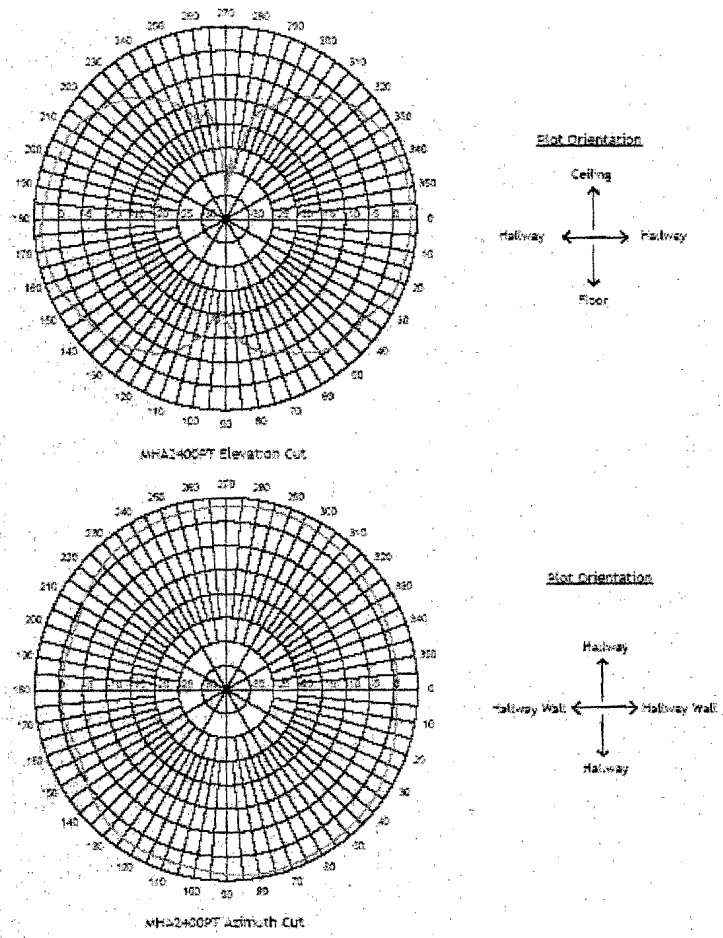


Figura 4 Patrón de radiación de la antena MHA2400PT

Standards:
- IEEE 802.3, IEEE 802.3u, IEEE 802.11b and IEEE 802.11g

Protocols:
- DHCP (Client), TCP/IP, IPX/SPX, NetBEUI

Module Technique:
- 802.11b: CCK, DQPSK, DBPSK; 802.11g: OFDM

Media Access Protocol:
- CSMA/CA with ACK

Frequency Range:
- 2.4 ~ 2.4835 GHz

Data Rate (auto fallback):
- 802.11b: 11Mbps, 5.5Mbps, 2Mbps, and 1Mbps
- 802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps and 6Mbps

Channels:
- 11 Channels (US Version), 13 Channels (EU Version)

Security:
- 64/128-Bit WEP, WPA (TKIP, AES) and MAC Address Access Control (ACL)

Antenna Connector:
- Male Reverse SMA Connector

Antenna:
- 3dBi Detachable Dipole Antenna

Output Power:
- 15 dBm, 1dBm

Receiving Sensitivity:
- 11Mbps 10 ~ 5 BER @ -80 dBm (typical)
- 54Mbps 10 ~ 5 BER @ -65 dBm (typical)

Management:
- HTTP, SNMP v1, v2

Ethernet Port:
- UTP/STP RJ-45, 10/100Mbps, Half/Full Duplex, Auto-MDIX

LED Indicators:
- Power, Link, Active

Power Adapter:
- Input: 100~240VAC, 0.35A, 50~60Hz
- Output: 4.7V ~ 5.3V VDC, 2A

Dimensions (LxWxH):
- 142 x 101 x 36.9 mm (5.6 x 4 x 1.45 inches)

Weight:
- 330 g. (11.6 oz.)

Temperature:
- Operating: 0°~ 40°C (32°F~104°F)

Humidity:
- Max. 90% (non-condensing)

Certification:
- FCC, CE

TEW-410APBplus

Tabla 4 Datos técnicos del Punto de acceso TEW-410APBplus

FIBER OPTIC CABLES 107

Heavy-Duty, Double-Jacket Cable

Loose Tube — Outdoor

Product Specifications

Fiber Counts	2 through 36
Fiber Size	50µm, 62.5µm
Buffer Tube Diameter	2.5mm
Strength Members	Dielectric Central Member, Fiberglass Yarn
Jacket Material	Medium-density Polyethylene (MDPE)
Temperature Range	
Storage	-40 to +80°C
Operating	-40 to +80°C

Fiber Specifications

	Multimode	
	50µm	62.5µm
Max. Attenuation (dB/km @850/1300nm)	3.5/1.0	3.5/1.0
Min. Bandwidth (MHz-km @850/1300nm)	500/500	220/500
Max. Gigabit Ethernet Distance (m)	600/600	300/550
Numerical Aperture	0.20	0.275

Part No.	Fiber Count	Cable Diameter (mm)		Weight (kg/km)		Tensile Strength (N)		Crush Resistance (N/cm)	
		Nom.	Max.	Nom.	Max.	Long Term	Short Term	Long Term	Short Term
MLD6002	2	.522	13.3	80	119	600	2666	180	800
MLD6004	4	.522	13.3	80	119	600	2666	180	800
MLD6006	6	.522	13.3	80	119	600	2666	180	800
MLD6008	8	.522	13.3	80	119	600	2666	180	800
MLD6012	12	.522	13.3	80	119	600	2666	180	800
MLD6018	18	.522	13.3	80	119	600	2666	180	800
MLD6024	24	.522	13.3	80	119	600	2666	180	800
MLD6036	36	.522	13.3	80	119	600	2666	180	800

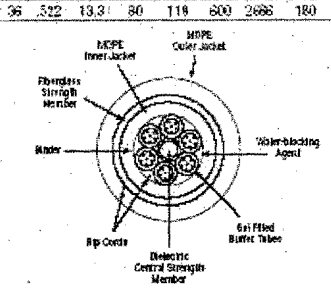


Tabla 5 Datos técnicos de la fibra óptica

Description	Part No.	UL Type/ CSA(1) Type	No. of Pairs	Nominal Weight		Nominal Diameter Over Jacket		Insulation Thickness		Nominal DCR		Mutual Capacitance @ 1kHz	Nom. Velocity of Propagation	Nom. Delay	Max. Attenuation @ 1 MHz	Max. Attenuation @ 4 MHz	Min. Pair to Pair NEXT @ 1 MHz	Min. Pair to Pair NEXT @ 4 MHz	Min. ACR @ 1 MHz (dB)	Min. ACR @ 4 MHz (dB)
				ft	m	in	mm	in	mm	Ω/km	Ω/kft	pF/ft	%	ns/100 m	dB/100 m	dB/100 m	dB/100 m	dB/100 m		
Non-Plenum / Polyolefin Insulation / PVC Jacket (Available in White, Black, Dark Gray, Blue, Red, Orange, Yellow, Green or Pink)																				
	1583A	NEC:	4	U-1000	U-304.8	21.0	9.6	.008	.20	.214	5.44	9.38	5.0	330	1	2.0	62.3	60.0	60.8	100±15	20.0
		CM		1000	304.8	21.0	9.6								4	4.1	53.3	49.0	48.7	100±15	23.0
		CEC:		1640†	500.0	34.4	15.7								10	6.6	47.3	41.0	40.8	100±15	25.0
		CM		3000†	914.4	63.0	28.6								16	8.2	44.3	36.0	36.7	100±15	25.0
															31.25	11.7	39.9	28.0	30.9	100±15	23.6
															62.5	17.0	35.4	19.0	24.8	100±15	21.5
															100	22.0	32.3	11.0	20.8	100±15	20.1
															200	32.0	27.8	1.0	14.7	100±25	15.0
Rip Cord																				
	1583R	NEC:	4	U-1000††	U-304.8	22.0	10.0													
		CMR		1000††	304.8	22.0	10.0													
		CEC: CMR FT4		3000††	914.4	66.0	30.0													

†1640 ft. pull-up available in Dark Gray or Blue only. 3000 ft. pull-up available in Dark Gray, White or Blue only.
††U-1000 ft. and 1000 ft. pull-ups not available in Black. 3000 ft. pull-ups available in Dark Gray, White or Blue only.
Jacket sequentially marked at 2 ft. intervals.
Third party verified to TIA/EIA-568-B.2, Category 5e

Tabla 6 Datos técnicos del cable UTP

Glosario

1000Base-LX Especificación para gigabit Ethernet en fibra óptica multi modo y mono modo con láser de onda larga.

1000Base-SX Especificación para gigabit Ethernet en fibra óptica multimodo y láser de onda corta.

1000Base-T Especificación para gigabit Ethernet sobre cable UTP categoría 5.

100BaseTx, Red de área local capaz de transmitir datos a 100 mbps a través de cable trenzado, el termino es sinónimo de Fast Ethernet

10BaseFx, Estándar IEEE para Ethernet de banda base a 10 Mbps sobre fibra óptica

10BaseTx, Red de área local Ethernet capaz de transmitir datos a 10 mbps a través de de cableado de par trenzado.

802.11, Es un tipo de tecnología de radio usado para redes de área local inalámbricas (WLAN). Es un estándar que ha sido desarrollado por el IEEE. El subgrupo 802 (del IEEE) desarrolla estándares para redes de área local y amplía con la sección 802.11 revisando y creando estándares para redes de área local inalámbrica.

802.11, Estándar IEEE que especifica el acceso al medio y las especificaciones de la capa física. Para conectividad inalámbrica a 1 y 2 Mbps entre estaciones fijas, portátiles y estaciones móviles dentro de un área local.

802.11a, Una revisión del estándar que opera en la banda de 5 GHz. La mayoría de los productos 802.11a, tienen velocidades de transmisión de datos de hasta 54 Mbps.

802.11b, Una revisión de el estándar IEEE para redes LAN inalámbricas con DSSS (secuencia directa/espectro disperso). La mayoría de los dispositivos 802.11b tienen velocidades de hasta 11 Mbps en la banda de 2.4 GHz.

802.11g, Similar al 802.11b, pero este estándar proporcionan una velocidad de transferencia de información de 54 mbps. También opera en la banda de frecuencia de 2.4 GHz pero usa diferente tecnología de radio en orden de estimular el ancho de banda total.

802.1d, Ver spanning tree protocol.

802.1x, Implementación de seguridad en redes inalámbricas, significando un incremento en la seguridad en la autenticación de usuarios usando RADIUS, protocolo de autenticación extensible (EAP), y LDAP para autenticación basada en puertos entre un sistema operativo y un dispositivo de acceso a la red.

802.2, Estándar IEEE que especifica el control de enlace lógico (LLC) que es común en todas las series LAN 802.

802.3, Estándar IEEE que especifica el control de acceso al medio por detección de portadora y las especificaciones de la capa física para redes LAN por cable a 10 Mbps.

802.3ab, Estándar para Ethernet a 1000 Mbps sobre par de cobre trenzado.

802.3u, Estándar de la IEEE que especifica ethernet a 100 Mbps sobre par de cobre trenzado.

802.3z, Estándar para ethernet a 1000 Mbps sobre fibra óptica.

802.5, Estándar IEEE que especifica el método de acceso al anillo pasando una estafeta para redes LAN por cable.

Access point, Punto de acceso, un dispositivo de capa 2 que sirve como interfaz entre la red inalámbrica y la red por cable, y puede controlar el acceso al medio usando RTS/CTS. Los access point combinados con un sistema de distribución (ejemplo Ethernet) soportan la creación de múltiples células de radio (BSSs) que permiten la facilidad del Roaming.

ACK, Abreviatura usada por lo común para el mensaje de reconocimiento utilizado en operaciones de acuerdo de conexión entre dos dispositivos de comunicación.

ADC, Convertidor analógico-digital. Convertidor que únicamente representa todas los valores de entrada analógicas. Dentro de un específico rango de entradas totales por un limitado numero de códigos de salida digital.

Ad-Hoc modo, Un cliente configurado que proporciona conectividad independiente punto-punto un una LAN inalámbrica de cliente a cliente, sin la intervención de un punto de acceso.

ADSL, Línea suscriptora digital asimétrica. Un método para incrementar la velocidad de transmisión en un cable de cobre. ADSL facilita la división de la capacidad en un canal con alta velocidad al suscriptor, típicamente para transmisión de video, y una canal con significativamente baja velocidad en la otra dirección.

AES, Estándar de encriptación avanzada. Usa el algoritmo Rijnadael y fue seleccionado por el Instituto de estándares e información nacional (NIST) como el estándar de procesamiento de información federal (FIPS) y hasta la fecha es considerado como indescifrable.

AGC, Control de ganancia automática. Sistema que sostiene la ganancia y de acuerdo con el rendimiento de un receptor sustancialmente constante a pesar de la fluctuaciones de la amplitud de la señal de entrada.

Aliasing, Un tipo de distorsión de la señal que ocurre cuando frecuencias de muestreo de una señal es menor que la razón de Nyquist.

AM, Modulación por amplitud de la señal eléctrica., AM, Modulación en amplitud, Modulación de onda continúa usando variación de la amplitud de la señal en proporción de la amplitud de una señal moduladora, usualmente tomada como DSB-LC para transmisión de broadcast comercial y DSB-SC para sistemas multiplexados.

Amplificador, Es un dispositivo que permite incrementar el nivel de una señal por un extremo llega la señal original y a la salida del amplificador sale una señal que es mucho mayor a la señal de entrada.

Analógico, Basado en valores de voltaje que varían continuamente.

Ancho de banda, Medida de la cantidad de información que fluye a través de un canal de comunicación en una unidad de tiempo determinada. Para dispositivos digitales se mide en bits por segundo.

Ancho de haz de la antena, Más apropiadamente referido como la potencia media de ancho del haz, esta es el ángulo de un patrón de antena o haz sobre el que la potencia relativa es cerca de 50 % de la potencia pico.

Antena, Es un dispositivo o estructura usado para recibir o radiar ondas electromagnéticas. La parte de los sistemas de transmisión designado para radiar o recibir ondas electromagnéticas.

ARP, Protocolo de resolución de direcciones, Protocolo de capa 3 que se utiliza para ligar una dirección IP a una dirección MAC definido en el RFC826.

Atenuación, Un término usado para describir la disminución de la amplitud de una señal de RF debido a la resistencia de cables conectores, divisores u obstáculos encontrados en la trayectoria de la señal.

ATM, Modo de transferencia asíncrona, Una tecnología para transmisión de banda ancha para señales de telecomunicaciones de alta capacidad. En adición a la transmisión de señal de alta capacidad, ATM proporciona flexibilidad considerable, desde el suscriptor individual es capaz de adaptar la capacidad de la conexión conmutada a sus requerimientos actuales.

Autenticación, ES el proceso que usa una estación para anunciar su identidad a otra estación. El estándar 802.11 especifica dos formas de autenticación: sistema abierto y clave compartida.

Backbone, Una línea de alta velocidad o una serie de conexiones que forman un mayor ancho de banda en una red. La parte central de una red grande que enlaza dos o más subredes y es la principal ruta para la transmisión de datos

Banda base, Método de comunicación en donde la señal de transferencia de información se coloca directamente en el cable en forma digital y sin modulación, su instalación es más económica que las redes de banda ancha que requieren de cable coaxial

BER, (Bit error rate), razón de errores de bit en un tiempo determinado.

Bit, (Binary Digit) Un solo dígito o número en base-2, en otras palabras, es o un 1 ó un cero. La unidad más pequeña de almacenamiento de datos en un sistema computarizado. El ancho de banda (Bandwidth) es comúnmente medido en bits- por- segundo.

Bits por Segundo, bps, Una medición de la velocidad de transmisión de datos sobre líneas de comunicación, basados en el número de bits que pueden ser enviados o recibidos por Segundo.

Bluetooth, Es una tecnología de salto de frecuencia en la banda de los 2.4 ghz y con un rango de 30 pies (aproximadamente 10 metros).

BPSK, Switcheo por cambio de fase binaria

Bridge (Puente), Un producto que conecta una red de área local a otra red de área local que usa el mismo protocolo (por ejemplo wireless, Ethernet o token ring). Wireless bridge son comúnmente usados para enlazar edificios en campus.

Broadband, Banda ancha, Una conexión comparativamente rápida a Internet. Servicios tales como ISDN, cable MODEM, DSL y satélite son todos considerados Broadband. No hay una definición oficial de la velocidad de Broadband, pero los servicios de 100 kbps y superiores son considerados como Broadband.

Byte, Un conjunto de Bits, números binarios que representan un solo carácter. Comúnmente son 8 bits en un byte.

Cable Crossover, Un cable especial para interconectar dos computadoras sin el uso de un hub. Los cables crossover pueden también ser requeridos para conectar un cable MODEM o un MODEM DSL a un Gateway inalámbrico o access point. El cambio de la transferencia de señal en rutas paralelos desde un plug a otro.

Cable MODEM, Una clase de convertidor usado para conectar una computadora a los servicios de TV por cable que proporciona además acceso a Internet. La mayoría de los modems por cable tienen una salida Ethernet que entonces se conecta a un Gateway Wi-Fi.

CCA, Valoración de canal libre.

CCK, Switcheo de código complementario

CDMA, Acceso múltiple por división de código.

CHAP, Protocolo de autenticación de desafió de saludo (challenge handshake authentication protocol), es un tipo de autenticación en el cual el agente de autenticación (típicamente un servidor de red) envía al programa cliente una clave para ser usada para encriptar el nombre de usuario y el password. Esto permite a nombre de usuario y password ser encriptados para ser transmitidos en forma encriptada para protegerlos contra cualquier otro usuario ajeno a la comunicación.

Clave de encriptación, Una serie alfanumérica (letras y/o números) que habilitan a los datos para ser encriptados y entonces des encriptados y así pueden ser seguros de compartir con una cantidad de miembros de la res. WEP usa una clave de encriptación que automáticamente encripta

los datos de salida inalámbricos. En el lado receptor, la misma clave de encriptación permite a la computadora des encriptar automáticamente la información y así poder leerla.

Cliente, Software empleado para contactar y obtener información de otro software ubicado en un servidor de red de otra computadora, a menudo a grandes distancias. Cliente, una computadora conectada a una red que requiere servicios (archivos, impresoras) de otro miembro de la red.

CRC, Código de redundancia cíclica

CSMA/CA, Es el principal método de acceso al medio empleado por el IEEE 802.11 WLANs. Este es un método de "escuchar antes de hablar", para minimizar (pero no eliminar) las colisiones causadas por transmisiones simultaneas por múltiples radios. Es el método para evitar las colisiones en el 802.11 distinto a la detección de colisiones, debido a que el estándar emplea radios half-duplex, radios con capacidad de transmitir o recibir, pero no simultáneamente. Distinto a los nodos Ethernet convencionales alambrados, una estación WLAN no puede detectar una colisión mientras transmite. Si una colisión ocurre, la estación transmisora no recibirá un paquete de reconocimiento (ACK). Poe esta razón, los paquetes ACK tienen una alta prioridad en todos los tráficos de red. Después de la terminación de la transmisión de datos, la estación receptora empezara transmitiendo un paquete ACK entes de que cualquier otro nodo pueda empezar a transmitir un nuevo paquete de datos. Todas las demás estaciones deberán esperar un tiempo aleatorio largo antes de transmitir. Si un paquete ACK no es recibido, la estación transmisora espera por una subsiguiente oportunidad para reintentar transmitir.

CSMA/CD, Un método para administrar el tráfico y reducir el ruido en una red Ethernet. Un dispositivo de red transmite datos después que detecta un canal disponible. Sin embargo, si dos dispositivos transmiten datos simultáneamente, los dispositivos que envían detectan una colisión y retransmiten después de un tiempo aleatorio.

Decibel, Una unida de medición que representa la diferencia entre dos niveles de señal. Poe ejemplo el incremento de potencia debido a un dispositivo activo tales como un amplificador o la disminución de la potencia debido a un dispositivo pasivo tales como un atenuador o un cable.

DHCP, Una utilidad que habilita un servidor para asignar dinámicamente direcciones IP desde una lista predefinida y limita el tiempo de uso que ella puede ser asignada. Sin DHCP, un administrador de IT deberá ingresar manualmente todas las direcciones IP en todas las

computadoras de la red. Cuando Dial-up, Una conexión de comunicación vía el estándar de la red telefónica, POTS (Plain old telephone service).

Directividad de antena, Esta es una ganancia relativa del patrón de un haz principal de una antena para referirse a una antena, usualmente isotropica o dipolo estándar.

Dispositivos de cliente, Los clientes son los usuarios. Los dispositivos clientes Wi-Fi incluyen tarjetas de de PC que se deslizan dentro de la computadora portátil, módulos mini-PCI instalados dentro de estas y dispositivos de computo móvil, como radios USB y radios Wi-Fi de bus PCI/ISA. Los dispositivos clientes usualmente se comunican con un dispositivo hub como un access point y un Gateway.

Diversidad de antena, Un tipo de sistema de antenas que usa dos antenas para maximizar la calida de la recepción y transmisión y reducir la interferencia sobre señales de multi-trayectoria.

DMZ, Zona des-militarizada, Ubicación fuera de la seguridad que brinda un firewall.

DNS, Un programa que traslada URLs hacia direcciones IP a través del acceso a una base de datos que mantiene una colección de servidores de Internet. El programa trabaja atrás del escenario para facilitar la navegación en la web con palabras contra direcciones numéricas. Un servidor DNS convierte un nombre como mywebsite.com a una serie de números como 107.22.55.26. Cada website tiene su propia dirección IP en el Internet.

DoS, Negación de servicio.

DQPSK, Switcheo por cambio de fase en cuadratura diferencial

DS, Secuencia directa

DSL, Protocolos de tecnología para datos a alta velocidad, voz y transmisión de video sobre una línea telefonía alambrada ordinaria de par trenzado de cobre POTS.

DSSS, Espectro disperso de secuencia directa

DSSS, Espectro disperso de secuencia directa, combina los datos que envía una estación con una secuencia de bits de alta velocidad, a los cual muchos se refieren como la secuencia de chips, también conocida como el proceso de ganancia el proceso de ganancia incrementa la resistencia de la señal a la interferencia.

E-mail, Correo electrónico, mensajes, comúnmente texto, enviado por una persona a otra a través de la computadora. El correo electrónico (e-mail) puede ser también enviado automáticamente y simultáneamente a un número mayor de direcciones (lista de correos).

Escaneo activo, Método por el cual las estaciones transmiten un frame de prueba y todos los puntos de acceso dentro del rango responden con un frame de respuesta de prueba, similar al escaneo pasivo, la estación seguirá la pista de la respuesta de prueba y tomara la decisión de a cual punto de acceso se autenticara y asociara con base en la repuesta de prueba que tenga el nivel de la señal más fuerte.

ESSID, Es el identificador del conjunto de servicios extendidos de un punto de acceso.

Ethernet, Un método muy común de establecer redes en una LAN (red no muy grande "local área network) Ethernet maneja aproximadamente 10, 000,000 bits – por –segundo y puede ser usado con casi todo tipo de computadora.

Evitar colisiones (CA), Una característica de un nodo de red para detección pro-activa que puede transmitir una señal sin riesgos de colisión.

FCS, Secuencia de chequeo de frame

FFT, Transformada rápida de fourier

FH, Salto de frecuencia

FHSS, Espectro disperso de salto de frecuencia

Fibra óptica, Cable de fibra de vidrio que transporta señales de luz láser o de luz LED para redes de computadoras.

Firewall, Una combinación de hardware y software que separa una LAN (local área network) en dos o más partes por motivos de seguridad. Los firewall bloquean cierto tipo de tráfico que es considerado como de riesgo, permitiendo protección contra ataques hechos a otros recursos de la red tales como archivos sensitivos, bases de datos y aplicaciones.

FTP, (File Transfer Protocol) Un método muy común de transferir archivos a través de sitios de Internet. Es una manera especial de establecer contacto (login) con otros sitios Internet con propósito de obtener ó enviar archivos.

FWT, Transformada rápida de Walsh

Gateway, El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles, por ejemplo Prodigy tiene un gateway que traduce su formato interno de correo electrónico al formato Internet del e-mail. Otro significado menos correcto de gateway es el describir cualquier mecanismo para proveer acceso a otro sistema por ejemplo, AOL puede ser llamado un gateway hacia Internet.

Half-duplex, Comunicación semi-duplex, solo en un sentido a la vez.

Host, Cualquier computadora en una red que es fuente de servicios disponibles a otras computadoras en cierta red. Es muy común el tener una máquina host que provee diversos servicios, tal como WWW y USENET.

HotSpot, Un lugar donde podemos accesar a los servicios de Wi-Fi. Este puede ser gratis o de paga y puede estar dentro de una tienda, una café, un hotel o un área publica.

Hub, Es un dispositivos multi-puerto usado para conectar computadoras a una red a través de cableado ethernet o Wi-Fi. Un hub transmite los paquetes que recibe en todos los puertos conectados.

Hz, Unidad de medición internacional para la medición de la frecuencia de una señal.

ICMP, Protocolo de mensajes de control de Internet.

Internet, La basta colección de redes interconectadas que emplean en general protocolos que emergen del ARPANET a finales de los 60´s y principios de los 90´s. Internet es ahora (Julio 1995) una gran conexión que tiene aproximadamente un mínimo de 60,000 redes independientes en todo el mundo creando una gran red global. Internet (minúscula) Cualquier vez que se conecten 2 o más redes (networks), se tiene un Internet-como inter-nacional ó inter-estatal.

Intranet, Una red privada dentro de una organización que emplea el mismo tipo de software que se encontrara en la red pública Internet, pero es de uso interno exclusivamente. A medida que Internet se ha hecho más famoso, muchas de las herramientas empleadas en Internet están siendo empleadas ahora en redes privadas, por ejemplo, muchas compañías tienen servidores de red que están disponibles solo para sus empleados y/o clientes.

IP, (Internet Protocol) protocolo de Internet utilizado en la capa tres de red. Asigna direcciones a los dispositivos de red.

IP dirección, A menudo llamado "dotted quad". Es un número único que consiste en cuatro partes separadas por puntos. Ejemplo: 165.113.245.2. Cada máquina que esta en Internet tiene un número único IP.

ISDN, (Integrated Services Digital Network) Básicamente es la manera de mover datos en líneas telefónicas regulares. ISDN esta siendo rápidamente disponible a la mayoría de Estados Unidos y en muchos mercados esta costeando muy similarmente a circuitos estándar analógicos. Provee una velocidad mínima de 128,000 bits – por – segundo en líneas telefónicas regulares. En la práctica, la mayoría de las personas serán limitadas a 56,000 ó 64,000 bps.

ISM, Banda industrial, médica y científica, banda de frecuencia que la FCC autoriza para las LAN inalámbricas. La banda ISM esta localizada en 915 +/- 13 MHz, 2450 +/- 50 MHz y 5800 +/- 75 MHz.

ISP, (Internet Service Provider) Una institución que provee acceso a Internet de alguna forma con intenciones lucrativas.

Kbps, Miles de bit por segundo.

Kerberos, Mecanismo de autenticación basada en etiquetas

Kilobyte, Mil bytes. Comúnmente ahora son 1024 (2 –10) bytes.

L2TP, Protocolo de túnel de capa dos.

LAN, (Local Área Network) Una red de computadoras limitados por el área que rodea a la red, comúnmente un edificio un piso de un edificio.

Ley A, Un tipo de cuantización no lineal (logarítmica), compresión expansión y técnicas de codificación para señales de voz basadas en la ley-A, este tipo de compresión expansión es usado internacionalmente y tiene similar respuesta como la ley-μ excepto que es optimizada para proporcionar una más cercana señal constante en la razón señal a ruido cuantificado, a costo de algún rango dinámico.

MAC, Control de acceso al medio, todas las tarjetas de red inalámbricas disponen de una dirección MAC para poder ser identificadas dentro de un entorno de red.

Mbps, Millones de bit por segundo

MDI/MDI-X, Interfaz dependiente del medio.

Megabyte, Un millón de bytes.

MODEM, (MOdulator, DEModulator) Un dispositivo que conecta una computadora a una línea telefónica y permite a la computadora comunicarse con otras computadoras mediante el sistema telefónico. Básicamente, los módem son para las computadoras como los teléfonos para los humanos.

Modo asíncrono, Una manera de envió de transmisión por inicial y paro de transmisión con un código en lugar de envió de transmisión de intervalo de tiempo especifico como en el modo sincrono. Los dispositivos de comunicación asíncronos no tienen que ser sincronizados con una señal de reloj, que es requerido con transmisión sincronía. También frecuentemente referido como ATM o modo de transferencia asíncrona. Puede también significar que hay diferentes capacidades para la transferencia de datos en cada dirección, por ejemplo los nuevos ADSL.

Modulo de potencia DC, Modulo que convierte potencia eléctrica AC a DC. Módulos de potencia sobre Ethernet de nivel empresarial que inyectan potencia sobre cables Ethernet conectan puntos de acceso.

MPDU, Unidades de datos del protocolo MAC

NAT, Traducción de direcciones de red, utilizado dentro de router para acceso a Internet.

NIC, Una tarjeta adaptadora de red que permite a un cliente conectarse a la red local y con la cual puede enviar y recibir información.

Nodo, Cualquier computadora por si sola conectada a una red.

Nombre de dominio, El nombre único que identifica un sitio de Internet. El nombre de dominio siempre tiene dos o más partes, separadas por puntos. La parte de la izquierda es la más especifica, la de la derecha es la más general. Una máquina podrá tener más de un nombre de domino. Cada nombre de dominio no se puede referir a más de una sola máquina.

OFDM, Multiplexión por división de frecuencia ortogonal.

OSI, Modelo de referencia de interconexión de sistema abierto.

OSPF, Abrir la ruta más corta primero, protocolo de ruteo utilizado dentro de los dispositivos que enlutan paquetes de datos.

Packet Switching, El método empleado para transportar datos en Internet, toda la información proveniente de una máquina es dividida en pedazos y cada uno de estos tiene una dirección hacia donde se dirige y hacia donde va. Esto permite a los pedazos de información de distintos lugares mezclarse en la misma línea, es por eso que varias personas pueden usar simultáneamente una sola línea.

Password (contraseña), Un código empleado para tener acceso aun sistema restringido. Las contraseñas más efectivas contienen letras y números con siete dígitos.

PC, Computadora de escritorio

PDA, Dispositivo portátil de mano con capacidades reducidas de cómputo.

PDH, Señal de jerarquía digital pleo-sincrona.

PHY, Capa física.

PKI, Integridad de clave publica.

PLCP, Protocolo de convergencia de capa física

Puerto, Un lugar donde la información entra o sale de una computadora. (ej.: puerto serial). En Internet un puerto se refiere a un número que es parte de un URL, y aparece después del colón (:) después del Domain Name. Cada servicio en servidores Internet en lista un número estándar de un puerto por ejemplo, los servidores de red normalmente tienen el puerto 80. Los servicios pueden ser también enlistados en puertos no estándar, este es el caso donde el puerto debe estar especificado en un URL cuando se accesa al servidor.

POTS, Estándar para los servicios de telefonía analógica

PPDU, unidad de datos del protocolo PLCP

PPP, Protocolo de punto-punto. El protocolo conocido como aquel que permite a una computadora el usar un teléfono común y un módem para hacer conexiones TCP/IP y entonces accesar Internet.

PPPoE, Protocolo de punto-punto sobre Ethernet.

PPTP, Protocolo de túnel de punto-punto.

PSTN, Red telefónica conmutada publica.

QPSK, Switcheo por cambio de fase en cuadratura

RADIUS, Servicios de usuario de marcación de acceso remoto, es un estándar para la autenticación de usuarios dentro de una red.

Red Ad hoc, Una red inalámbrica compuesta solo de estaciones sin punto de acceso.

Red, (Network) Cualquier vez que se conecten 2 o más computadoras de tal manera que puedan compartir recursos, se tiene entonces una red. Si se conectan 2 o más redes y se tienen una Internet.

RFC, Requerimiento para comentario.

RIP, Protocolo de información de ruteo.

RJ-45, Conector estándar utilizado para las redes Ethernet, similar al RJ-11 pero con ocho conexiones.

Roaming, La habilidad de un cliente inalámbrico para desconectar y conectarse de un punto de acceso a otro sin la intervención del usuario.

Router, (ruteador) Una computadora o software específico que maneja la conexión entre dos o más redes. Los ruteadores pasan todo el tiempo observando las direcciones de destino de los paquetes que pasan por ellos y deciden por que ruta serán enviados.

SDH, Señal de jerarquía digital sincrona

Server, (Servidor) Una computadora, o un paquete de software, que provee un tipo específico de servicio a un software de cliente ubicado en otras computadoras. Un solo servidor puede contener distintos tipos de paquetes de software corriendo, esto provee muchos servidores a los clientes de la red.

Servicios de asociación, Un servicio IEEE 802.11 que permite el mapeo de estaciones inalámbricas a un sistema distribuido vía el punto de acceso.

Site survey, El proceso mediante el cual se realiza una inspección al sitio donde se va a realizar la instalación de una red, o conjunto de equipos de telecomunicaciones.

SMA, Conector sub-miniatura de RF utilizado en radiocomunicaciones.

SMTP, Protocolo de transporte de correo simple.

SOHO, Termino utilizado para describir "pequeña oficina/oficina de casa.

SS, Espectro disperso.

SSID, También conocido como ESSID, identificador del conjunto de servicios.

SSL, Capa de seguridad de socket. Utiliza esquemas de encriptación basados en RC4. Es utilizado ampliamente en las transacciones comerciales a través de Internet.

STA, Estación

STP, Par de cobre torcido con blindaje.

Subnetwork o Subnet, Pequeñas redes que son usadas para simplificar el direccionamiento entre numerosas computadoras.

Switch, Un dispositivo concentrador que reemplazo a los tradicionales hub, con la ventaja de que solo envía los paquetes hacia el puerto que debe recibir la información, permitiendo la optimización de la red.

T-1, Una línea arrendada o dedicada capaz de transferir datos a 1, 544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta

un megabyte en menos de 10 segundos. Un T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.

TCP, Protocolo de control de transporte, aplica en la capa de transporte de modelo de referencia OSI.

TCP/IP, (Transmission Control Protocol/Internet Protocol) El protocolo que mejor describe a Internet. Originalmente diseñado para sistemas operativos UNIX, el software TCP/IP es ahora disponible para cualquier sistema operativo mayor. Para poder tener una conexión a Internet una computadora requiere TCP/IP.

TDM, Múltiplex por división de tiempo.

TDMA, Acceso múltiple por división de tiempo.

Terminal Server, (Servidor terminal). Una computadora específica que permite conectar varios módems de uno de sus lados y una conexión a una red LAD o a otro servidor del otro lado. La mayoría de estos servidores proveen servicios PPP y SLIP si están conectados a Internet. Este servidor contesta llamadas en los módems y las transfiere a los nodos adecuados.

Terminal, Un dispositivo que permite enviar comandos a una computadora ubicada en otro lugar. Como mínimo esto es un teclado y una pantalla y un conjunto sencillo de circuitos. Comúnmente se usa el software de una terminal en una computadora personal.

TKIP, Protocolo de integridad de claves temporales.

UDP, Protocolo de datagramas de usuario.

UHF, Frecuencia ultra alta.

UTP, Par de cable torcido sin blindaje.

VHF, Frecuencia muy alta (very high frecuency

VoIP, Transmisión de voz sobre IP.

VPN, (Virtual private network) red privada virtual. Utiliza protocolos de autenticación y encriptación para realizar túneles a través de redes publicas como el Internet.

WAN, (Wide Área Network) Una red de computadoras que cubre un área mayor a un solo edificio, edificio o campus.

Watt, Unidad de medida de la potencia eléctrica, tiene sus múltiplos que son mW, KW, MW, etc.

WEP, Privacidad equivalente alambrada, es el nivel de encriptación más básico para redes WLAN basado en la encriptación RC4. Proporciona encriptación de 64 y 128 bits.

Wi-Fi, Organismo de certificación de interoperabilidad para redes inalámbricas LAN basados en el estándar 802.11.

Windows, Sistema operativo de Microsoft

Wireless, Inalámbrica

WLAN, Red inalámbrica de área local

WNIC, Tarjeta de interfaz de red inalámbrica.

WPA, Acceso protegido Wi-Fi, es un método de encriptación que protege de accesos no autorizados utilizando un conjunto de clave y nombre de usuario.

Zo, Impedancia característica de un dispositivo de radiocomunicación (antena, cables)

Zona de Fresnel, Es una zona con forma oval alrededor del lóbulo principal de una señal de RF, puede ser 60 a 80 % libre de obstáculos para asegurar la adecuada recepción de la señal entre dos dispositivos inalámbricos que hacen un enlace.

Bibliografía

Redes de computadoras, tercera edición

Autor, Andrew S. Tanenbaum

Editorial prentice hall

ISBN 968-880-958-6

Redes de computadoras, segunda edición

Autor, Uyless Black

Editorial Addison Wesley Iberoamericana

ISBN 0-201-87889-5

Tecnologías de inter conectividad de redes

Autor, Merilee Ford, Steve Spanier, Tim Stevenson

Editorial Prentice hall

ISBN 970-17-0171-2

Windows 2000 TCP/IP

Autor, Karanjit Siyan, PH.D

Editorial Prentice Hall

ISBN 84-205-2947-8

Digital microwave radio, technical information on NEC´s DMR

NEC Corporation, Tokio Japón

Wireless Maximum Security

Autor, Dr. Cyrus Peikari and Seth Fogie

Editorial Sams

ISBN 0-672-32488-1

Real 802.11 security

Autor, Jon Edney, William A. Arbaugh

Editorial Addison Wesley

ISBN 0-321-13620-9

Certified Wireless Network Administrator, official study guide

Autor Planet3 wireless

Editorial Mc Graw Hill

ISBN 0-07-222902-0

Certified Wireless Security Professional, official study guide

Autor Planet3 wireless

Editorial Mc Graw Hill

ISBN 0-07-223012-6

Windows server 2003

Autor, Mark Minasi

Editorial SYBEX

ISBN 0-7821-4130-7

Principles of communication systems

Autor Herbert Taub, Donald L. Schilling

Editorial Mc Graw Hill

ISBN 0-07-100313-4

Redes de computadoras, protocolos normas e interfaces

Autor: Uyless black

Editorial ra-ma

ISBN 0-201-87889-5

Introducción a los sistemas de comunicación

Autor F.G. Stremler

Editorial Addison-Wesley Iberoamericana

ISBN 0-201-51878-3

Introduction to Cisco networking Technologies

Autor Cisco press

Part # 97.1298-01

Interconnecting Cisco network devices

Autor Cisco press

Part # 97-1298-01

Decibel products catalog N0. 25

Autor Decibel products

Andrew catalog 36

Andrew

Referencias electrónicas

http://www.cisco.com

http://www.3com.com

http://www.intel.com

http://www.zdnet.com

http://www.webopedia.com

http://www.trendware.com

http://www.linksys.com

http://www.microsoft.com

http://www.telecomwriting.com

http://www.comptia.org/certification/

http://www.satelliteways.com/

http://www.dlink.com/

http://www.itt.com/

http://www.ieee802.org/1/pages/802.1Q.html

http://shop.ieee.org/ieeestore/

http://www.eia.org/

http://www.krone.com/

http://www.alepo.com/radius-billing.shtml

http://www.ofdmnews.com/publications/page207-586342.asp

http://www.pcmag.com/

http://www.freeradius.org/

http://www.microsoft.com/technet/default.mspx

http://www.80211info.com/

http://wireless.agilent.com/WLAN/mfg/ic.shtml

http://www.broadcom.com/products/category.php?category_id=40&cookiecheck=1

http://www.conexant.com/

http://grouper.ieee.org/groups/802/11/

http://www.netstumbler.com/

http://home.luna.nl/~arjan-muil/radio/history/history-frame.html

http://wlana.org/direct/wireless_semiconductor.html

http://sss-mag.com/

http://www.tiltek.com/

http://www.wi-fi.com/%20

http://telecomwriting.com

Se incluye CD con un archivo que contiene la tesis en formato PDF, el archivo se llama: TESIS_WLAN_VVIVEROS_2004.PDF.

Para abrir el archivo solo requieres el password "vviveros".