CAPITULO I

1. FUNDAMENTACION TEORICA DE LAS REDES INALAMBRICAS WLAN

1.1 Entorno De La Universidad Técnica De Cotopaxi

1.1.1 Antecedentes históricos

La Universidad Técnica de Cotopaxi, es una institución de Educación Superior Pública, Laica y Gratuita, creada mediante Ley promulgada en el Registro Oficial N.- 618 del 24 de enero de 1995, y que forma parte del Sistema Nacional de Educación Superior Ecuatoriano. Se rige por la Constitución Política del Estado, la Ley de la Educación Superior y otras leyes conexas. Es una institución universitaria sin fines de lucro que orienta su trabajo hacia los sectores urbanos, marginales y campesinos; que busca la verdad y la afirmación de la identidad nacional, y que asume con responsabilidad el aseguramiento de la libertad en la producción y difusión de los conocimientos y del pensamiento democrático y progresista para el desarrollo de la conciencia antiimperialista del pueblo.

En nuestra institución se forman actualmente profesionales al servicio del pueblo en las siguientes áreas de especialidades: Ciencias Exactas y Naturales, Ciencias Agropecuarias y Veterinarias, Ciencias Humanísticas y del Hombre. Realizamos esfuerzos para alcanzar cada día metas superiores y más competitivas, planteándonos como retos, la formación de profesionales integrales en los ámbitos de pre y postgrado al servicio de la sociedad, el desarrollo paulatino de la investigación científica y la vinculación con la colectividad a partir de proyectos generales y específicos, con la participación plena de todos sus estamentos. Somos una Universidad con adecuados niveles de pertinencia y calidad, logrados a través de la concientización y difusión de la

ciencia, cultura, arte y los conocimientos ancestrales. Contribuimos con una acción transformadora en la lucha por alcanzar una sociedad más justa equitativa y solidaria, para que el centro de atención del Estado sea el ser humano. Por ello, la Universidad Técnica de Cotopaxi asume su identidad con gran responsabilidad: "Por la vinculación de la universidad con el pueblo","Por una Universidad alternativa con Visión de Futuro" Consciente de sus avances e insuficiencias, la Universidad Técnica de Cotopaxi emprende decisivamente el camino hacia la trasformación plasmada en su Plan Estratégico de Desarrollo Institucional para el período 2003 – 2006.

1.1.2 Misión

La Universidad Técnica de Cotopaxi como entidad de derecho público y plena autonomía, plantea como Misión:

"Contribuir en la satisfacción de las demandas de formación y superación profesional, en el avance científico – tecnológico y en el desarrollo cultural universal y ancestral de la población ecuatoriana para lograr una sociedad solidaria, justa, equitativa y humanista. Para ello, desarrolla la actividad docente con niveles adecuados de calidad, brindando una oferta educativa alternativa en pregrado y posgrado, formando profesionales analíticos, críticos, investigadores, humanistas capaces de generar ciencia y tecnología. Asimismo, realiza una actividad científico – investigativa que le permite brindar aportes en la solución de los problemas más importantes de su radio de acción, y a través de la vinculación con la colectividad, potencia su trabajo extensionista. Se vincula con todos los sectores de la sociedad y especialmente, con aquellos de escasos recursos económicos, respetando todas las corrientes del pensamiento humano. La Universidad Técnica de Cotopaxi orienta sus esfuerzos hacia la búsqueda de mayores niveles de calidad, pertinencia y cooperación nacional e internacional, tratando de lograr niveles adecuados de eficiencia, eficacia y efectividad en su gestión. Se distingue de otras instituciones de educación superior de la provincia al ser una Universidad alternativa vinculada fuertemente al pueblo en todas sus actividades".

1.1.3 Visión de la Universidad

La Universidad Técnica de Cotopaxi plantea como Visión de Futuro los siguientes postulados que representan el estado mínimo deseable y posible de alcanzar:

- Se ha elevado la calidad de la formación integral profesional. Los graduados manifiestan satisfacción sobre la formación recibida en la mayoría de las carreras. Los Planes de Estudios y las Mallas Curriculares están actualizados. Crece ligeramente la oferta de carreras y especialidades, así como las modalidades de estudios.

- La matrícula en todas las carreras tiene un ligero aumento. Se eleva la promoción en los primeros dos ciclos en la mayoría de las carreras. Se amplía el número de alumnos – ayudantes y se apoya adecuadamente a los estudiantes de bajo rendimiento. Existe un mejor servicio en las bibliotecas a la comunidad universitaria, creciendo además el fondo bibliográfico para el pregrado y posgrado. Se refuerza el papel del Centro Experimental y de Producción de Salache con relación a la producción agropecuaria y la captación de recursos extrapresupuestarios.

- Se avanza ligeramente en el desarrollo de la investigación científica en cada una de las carreras, creciendo el número de proyectos en ejecución y los resultados en las áreas prioritarias definidas institucionalmente. Crece ligeramente el número de convenios en el área de la investigación. Se incrementan las cantidades de eventos científicos y de artículos publicados en la Revista Alma Mater. Crece el número de estudiantes que se incorpora a la investigación. El sistema de planificación y control de la investigación funciona adecuadamente. Mejora la infraestructura para desarrollar la investigación. Aumenta ligeramente la cantidad de recursos extrapresupuestarios captados a través de la investigación.

- Mejora la calidad de las actividades de posgrado. Crece ligeramente la oferta de maestrías, diplomados y estudios de doctorados en las áreas prioritarias definidas. Crece el número de Master en la planta docente. Se establecen convenios de cooperación con

Colegios Profesionales y otras Universidades para desarrollar actividades de posgrado. La actividad de posgrado se amplia a las ciudades en donde la Universidad posee Centros Asociados. La Dependencia Administrativa que atiende el posgrado en la UTC funciona eficientemente con el personal idóneo. Se logra incrementar el uso de las Nuevas Tecnologías de Información y Comunicación en las actividades de diplomados y maestrías.

- Se incrementan los Programas de Difusión Cultural, impactando favorablemente en los beneficiarios. Todas las carreras realizan actividades de extensión universitaria. El Servicio de Bienestar Universitario se amplía ligeramente y mejora la calidad de sus resultados. Se dispone de un Programa de Desarrollo de la Extensión Universitaria actualizado, que incluye la problemática del medio ambiente. Se alcanzan buenos resultados en la proyección del deporte hacia el sector externo. Se imparte actividades de superación sobre el área de extensión a los miembros de la comunidad universitaria. Se realizan actividades de educación continua y capacitación popular con buen impacto en los beneficiarios.

- El nivel de formación pedagógica, profesional y científica de los docentes aumenta. Se eleva ligeramente el número de docentes a tiempo completo. Se eleva el nivel preparación del personal administrativo, los empleados y las autoridades a través de actividades de capacitación y profesionalización contratadas al sector externo. El sistema de reclutamiento, selección, inducción y evaluación funciona adecuadamente. Se estimulan los mejores resultados del personal a través de un sistema de reconocimientos. Se incrementa el sentido de pertenencia a la Universidad por parte del personal.

- Se eleva la cultura informática de la comunidad universitaria. El nivel de preparación del personal en ésta área aumenta. Se alcanza una mayor cobertura en la satisfacción de las demandas de equipamiento de las diferentes áreas universitarias. Se

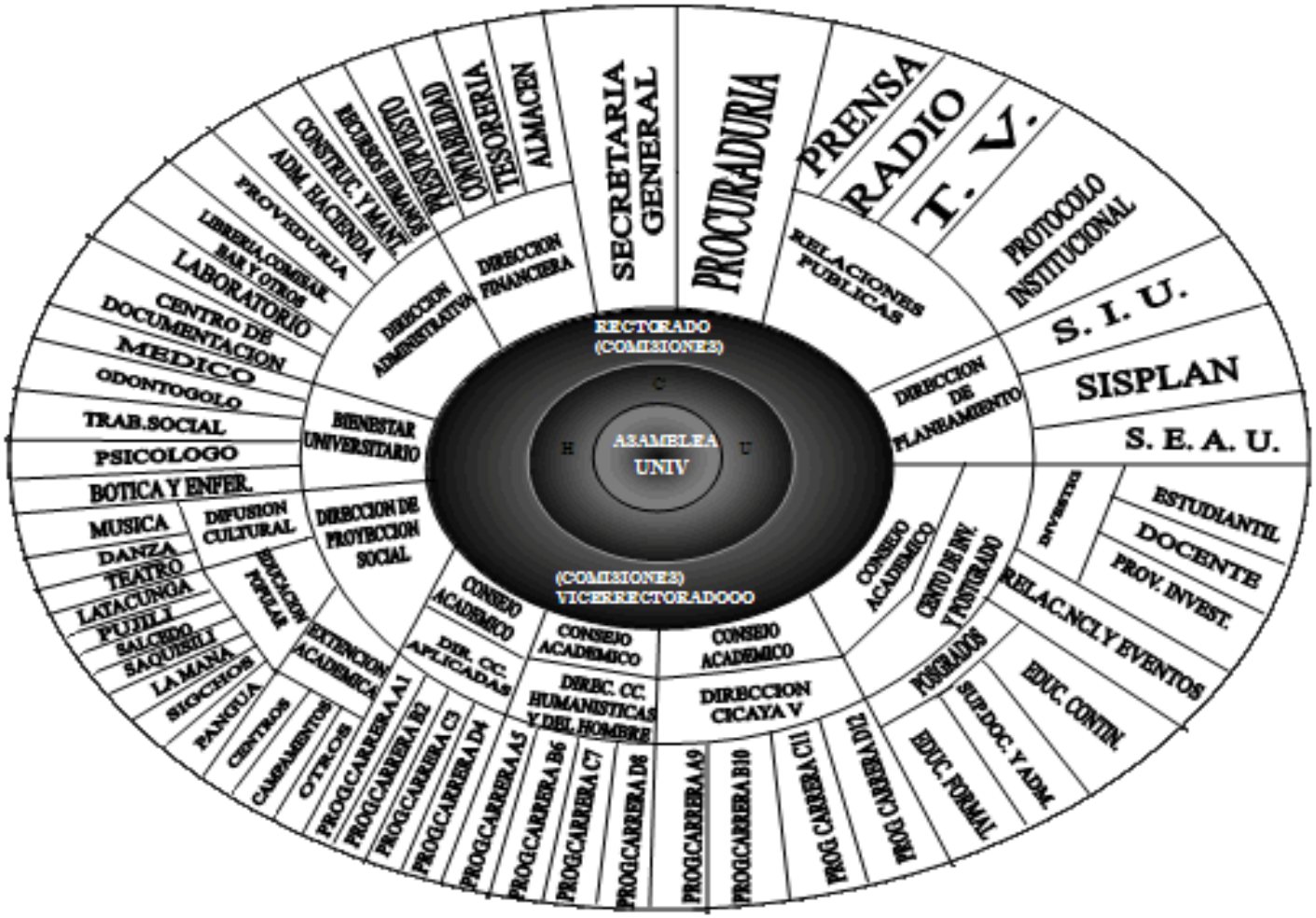
potencia el proceso de informatización de la Universidad con el aporte de los estudiantes.

- Se mejoran las relaciones con los colegios de bachillerato con mayor potencial de futuros aspirantes para la UTC, desarrollándose programas conjuntos. Se establecen alianzas estratégicas con algunas entidades productivas y de servicios y los Colegios Profesionales para realizar actividades conjuntas de mutuo beneficio. Aumenta el número de convenios con Universidades nacionales y extranjeras en áreas de interés institucional.
- Se dispone de un marco normativo actualizado y completo, que es conocido por la comunidad universitaria. Toda la base jurídica se encuentra bajo soporte automatizado.

- Mejora la gestión económica, financiera y administrativa universitaria. Se eleva el nivel de calificación del personal que trabaja en esas áreas y se automatizan una parte de los procesos, produciendo una disminución del tiempo para los trámites y una elevación de la eficiencia del personal. Se produce un incremento paulatino en la captación de fondos extrapresupuestarios de autogestión. Existe un uso más racional de los recursos disponibles. Se mejora ligeramente la remuneración salarial del personal. La disponibilidad y uso de la infraestructura física y del equipamiento crecen. Se obtienen buenos resultados en las auditorias internas y el control estatal.

- Se dispone de un nuevo módulo adicional del proyecto de Campus Universitario. El sistema de planificación institucional se fortalece; todas las dependencias elaboran anualmente su plan operativo. Se fortalece la Dirección por Objetivos en todas áreas universitarias. Se cuenta con un Sistema de Información Estadístico que contribuye favorablemente en la toma de decisiones. Se logra la acreditación de algunos programas académicos de pregrado y postgrado.

1.1.4 Estructura organizacional



1. 2 Sistemas de redes y tendencia a las telecomunicaciones

1.2.1 Introducción

Desde los albores de la humanidad, un tema fundamental con respecto al desarrollo y progreso, ha sido la necesidad de comunicación entre unos y otros, presente a lo largo de la historia. En los últimos años los nuevos logros de la tecnología han sido la aparición de computadores, líneas telefónicas, celulares, redes alámbricas e inalámbricas, así como las satelitales.

El principio de la comunicación se establece mediante el habla en la relación entre emisor, mensaje y receptor. Pero la tecnología de hoy en día no solo debe hacer referencia a la transmisión de voz, sino debe intentar abarcar una mayor gamma de aplicaciones, llámese la transmisión de datos. Dada esta necesidad es que surgen las redes de computadores como la intranet, la extranet y el internet. Referente al intercambio de voz y datos se hace indispensable la necesidad de estar conectados con el mundo entero a través de la Internet, de donde surgen algunos problemas concernientes a la aplicación de redes alámbricas debido a que se hace necesario el transporte de los equipos ya sea dentro de un local como al interior de alguna oficina.

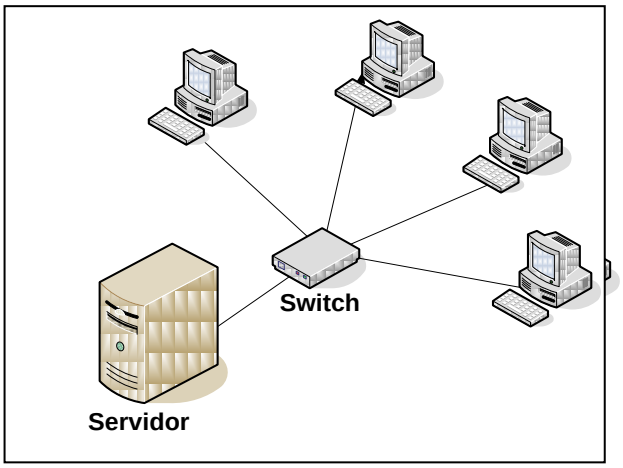
Al presentarse esta necesidad se hizo parte de un grupo de estudio de mayor envergadura, desde las redes inalámbricas, la transferencia de datos vía infrarrojo, así como en la aplicación de redes satelitales. Las mismas que han logrado satisfacer esta necesidad logrando la conexión de usuarios existentes en distintos lugares del mundo. La aplicación de la tecnología inalámbrica, viene teniendo un gran auge en velocidades de transmisión, aunque sin competir con la utilización de redes alámbricas o el uso de la fibra óptica, sin embargo cubren satisfactoriamente la necesidad del movimiento de los usuarios.

1.2.2 Definición de redes

"Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas".[1]

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

GRAFICO 1.1: REDES
FUENTE: GRUPO INVESTIGADOR



1.2.3 Definición de VLANs

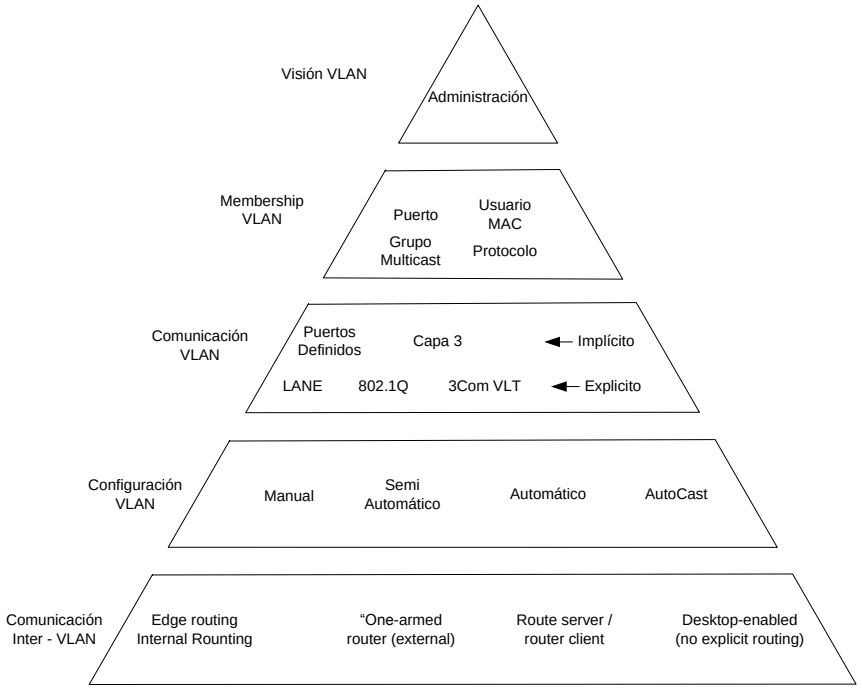
Las LANs virtuales (VLANs) son agrupaciones de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en

[1] RODRIGUEZ Jorge, Introducción a Las Redes De Área Local, McGraw Hill, México, 1998. Pág. 23-29

sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se están introduciendo en este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios.

Además, la red virtual simplifica el problema de administrar los movimientos, adiciones y cambios del usuario dentro de la empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del ratón del administrador de la red. Puesto que todos los cambios se realizan bajo control de software, los centros de cableado permanecen seguros y a salvo de interrupciones.

GRAFICO 1.2: ELEMENTOS DE LA IMPLEMENTACIÓN DE UNA VLAN.
FUENTE: WWW.EMAGISTER.COM/PUBLIC/PDF/COMUNIDAD_EMAGISTER/849677065484567-CONFIG-CISCOS.PDF



1.3. Elementos De Una Red Inalámbrica

Las redes locales inalámbricas se integran en una red privada igual que las otras redes locales. Por ejemplo, los puntos de acceso de la WLAN se conectan a un hub Ethernet y de éste a un encaminador IP.

1.3.1 Servidor

Es la máquina principal de la red. Se encarga de administrar los recursos de ésta y el flujo de la información. Algunos servidores son dedicados, es decir, realizan tareas específicas. Por ejemplo, un servidor de impresión está dedicado a imprimir; un servidor de comunicaciones controla el flujo de los datos, etcétera.

GRAFICO 1.3: SERVIDORES
FUENTE: REDES DE COMPUTADORAS. ANDREW TANENBAUM

Para que una máquina sea un servidor es necesario que sea una computadora de alto rendimiento en cuanto a velocidad, procesamiento y gran capacidad en disco duro u otros medios de almacenamiento.

1.3.1.1 Tipos de servidores

En la actualidad existen una variedad de servidores para múltiples aplicaciones, que son utilizadas por instituciones públicas y privadas en las cuales podemos citar los siguientes.

1.3.1.1.1 Servidor Web.

Básicamente, Un servidor Web es un computador preparado y acondicionado para estar permanentemente conectado a una red de alta velocidad. Esta red de alta velocidad forma parte de Internet, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML.

1.3.1.1.2 Servidores de Aplicaciones (*Application Servers*).

Designados a veces como un tipo de *middleware* (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan. "Los servidores de aplicación también brindan a los desarrolladores una Interfaz para Programación de Aplicaciones (API), de tal manera que no tengan que preocuparse por el sistema operativo". [2]

1.3.1.1.3 Servidores Proxy (Proxy Server).

Los servidores Proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

[2] http://wwww.monografias.com/trabajos18/redes-computadoras/redes-computadores.html

Funcionamiento

Un Proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. (Ejemplo: una página Web).

1.3.1.1.4 Servidor de Base de Datos

Los Servidores de Bases de datos (MySQL, ORACLE, etc) permiten aprovechar la estabilidad y seguridad que el sistema operativo Linux le ofrece para maximizar entre otros:

- Manejo de sus bases de datos ya sea desde el mismo servidor o desde sus aplicaciones remotas.
- Sincronización de sus bases de datos o la de sus clientes entre varios servidores.
- Configuración de varios motores de bases de datos de acuerdo con las necesidades particulares, ya sea para manejo interno o remoto.

1.3.1.1.5 Sistema operativo de red

Es el sistema que se encarga de administrar y controlar en forma general a la red: Linux Red Hat 4.0 Enterprise Server, Windows 2000 Advanced Server.

1.3.2 Terminales

Las terminales portátiles -usadas en aplicaciones de negocios- se pueden encontrar en diferentes formas y tamaños para resolver diversas tareas. Hoy en día en el ambiente dinámico de las empresas, la habilidad para manejar información en el punto de actividad ofrece a las compañías una ventaja competitiva. Ahora se cuenta con una

amplia variedad de productos con diferentes formas, sistemas operativos, opciones de comunicación, etc.

1.3.2.1 Clasificación de los terminales

Todas son una buena opción como herramienta de soporte ideal para el funcionamiento en el manejo de datos:

1.3.2.1.1 Key Based o Terminales basadas en teclado.

Cuando se tiene una aplicación de manejo de datos intensiva que requiere una entrada manual de la información, una Terminal portátil de captura de datos con teclado es la respuesta. Construida con un teclado alfanumérico fácil de usar y una pantalla iluminada. Para un alto rendimiento en comunicaciones existen opciones batch y radiofrecuencia.

1.3.2.1.2 Pen based o con pluma por contacto.

La gran diferencia con estas terminales con pluma por contacto es que no contienen teclado. La información se manipula simulando el uso de una pluma que por contacto permite introducir datos. Estas terminales incrementan la eficacia, efectividad y resisten el uso rudo en trabajo pesado suficiente para trabajar virtualmente en cualquier lugar. Es la herramienta indispensable para trabajadores en movimiento en todas las industrias donde se requiere que la información se recolecte donde sea generada. Como muchas otras terminales portátiles existen opciones batch y radiofrecuencia.

1.3.2.1.3 Montadas en un vehiculo

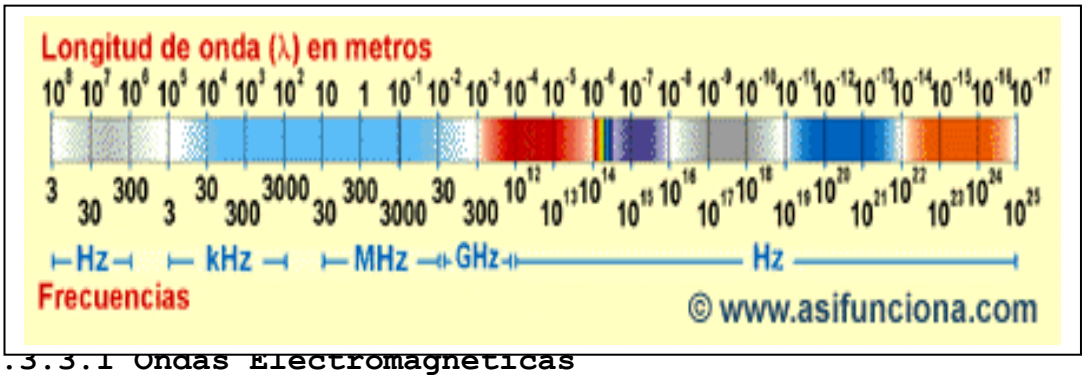
Cuando su necesidad sea contar con un dispositivo montado en un vehículo, como por ejemplo un montacargas, se cuenta con terminales para la industria móvil. Estas terminales permiten al operador capturar, procesar y comunicar la información

dondequiera que se encuentre; además pueden contener un lector de código de barras y permiten transmitir la información a un host remoto.

1.3.3 Espectro Electromagnético

Se denomina **espectro electromagnético** al conjunto de ondas electromagnéticas o, más concretamente, a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Van desde las de menor longitud de onda, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio.

GRAFICO 1.4: ESPECTRO ELECTROMAGNÉTICO.
FUENTE: WIKIPEDIA, LA ENCICLOPEDIA LIBRE.



1.3.3.1 Ondas Electromagnéticas

Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos. La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas).

1.3.3.1.1 Ondas de radio.

Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes: No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío. La velocidad es la misma que la de la luz, es decir 300.000 Km/seg. Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas.

GRAFICO 1.5: ONDAS DE RADIO
FUENTE: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.3.3.1.2 Microondas Terrestres

Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

GRAFICO 1.6: MICROONDAS TERRESTRES
FUENTE: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.3.3.1.3 Ondas Infrarrojas.

Llamadas también térmicas, llegan hasta la luz visible (el rojo del espectro), se producen por la vibración de los electrones de las capas superiores de ciertos elementos, estas ondas son absorbidas fácilmente por la mayoría de los materiales. La energía infrarroja que absorbe una sustancia aparece como calor, ya que la energía agita los átomos del cuerpo, e incrementa su movimiento de vibración o translación.

1.3.3.1.4 Ondas Visibles.

Son la parte del espectro electro-magnético que puede percibir el ojo humano. La luz se produce por la disposición que guardan los electrones en los átomos y moléculas. Las diferentes longitudes de onda se clasifican en colores que varían desde el violeta el de menor longitud de onda hasta el rojo el de mayor longitud de onda (de 4 a $7x10^{-7}$).

1.3.3.1.5 Ondas Ultravioletas.

Los átomos y moléculas sometidos a descargas eléctricas producen este tipo de radiación. No debemos de olvidar que la radiación ultravioleta es la componente principal de la radiación solar. La energía de los fotones de la radiación ultravioleta es del orden de la energía de activación de muchas reacciones químicas.

1.3.3.1.6 Rayos X.

Si se aceleran electrones y luego, se hacen chocar con una placa metálica, la radiación de frenado produce rayos X. Los rayos X se han utilizado en medicina desde el mismo

momento en que los descubrió Röntgen debido a que los huesos absorben mucho más radiación que los tejidos blandos.

1.3.3.2 Características de las Ondas Electromagnéticas

1.3.3.2.1 Frecuencia (f)

La frecuencia de una onda responde a un fenómeno físico que se repite cíclicamente un número determinado de veces durante un segundo de tiempo, tal como se puede observar en la siguiente ilustración:

TABLA 1.1: ESPECTRO DE LAS RADIACIONES DE LAS ONDAS ELECTROMAGNÉTICAS.
FUENTE: © 2002. CARLOS ANDRÉS CARVAJAL T. ASTRÓNOMO AUTODIDACTA.

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

1.3.3.2.2 Longitud (λ)

Las ondas del espectro electromagnético se propagan por el espacio de forma similar a como lo hace el agua cuando tiramos una piedra a un estanque, es decir, generando ondas a partir del punto donde cae la piedra y extendiéndose hasta la orilla.

1.3.3.2.3 Amplitud (A)

a amplitud constituye el valor máximo que puede alcanzar la cresta o pico de una onda. El punto de menor valor recibe el nombre de valle o vientre, mientras que el punto donde el valor se anula al pasar, se conoce como “nodo” o “cero”.

1.3.4 Medio Ambiente

Se entiende por **medioambiente** o **medio ambiente** al entorno que afecta y condiciona especialmente las circunstancias de vida de las personas o la sociedad en su conjunto. Comprende el conjunto de valores naturales, sociales y culturales existentes en un lugar y un momento determinado, que influyen en la vida del hombre y en las generaciones venideras. Es decir, no se trata sólo del espacio en el que se desarrolla la vida sino que también abarca seres vivos, objetos, agua, suelo, aire y las relaciones entre ellos, así como elementos tan intangibles como la cultura.

1.3.5 Switch Inalámbrico

El Switch inalámbrico WS2000 es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en sucursales. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión. La compatibilidad con extensiones Wi-Fi Multimedia (WMM) permite al WS2000 ofrecer el mejor rendimiento incluso en las aplicaciones más complejas con voz y vídeo.

GRAFICO 1.7: SWITCH INALÁMBRICO SYMBOL WS2000.
FUENTE: HTTP://WWW.ZETES.COM/ELINK/05Q1/SPAIN/WIRELESS-SWITCH.HTM.

1.3.6 Access Point

Un **punto de acceso inalámbrico** (**WAP** o **AP** por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red **ad-hoc**).”Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada”.[3]

GRAFICO 1.8: ACCES POINT.
FUENTE: HTTP://ES.WIKIPEDIA.ORG/WIKI/PUNTO_DE_ACCESO.

1.3.7 Tarjetas Inalámbricas

1.3.7.1 Características de las tarjetas inalámbricas más utilizadas en la auditoria wireless.

[3] http://www.pucelawireless.net/index.php?pagename=AccessPoint

Basándome en la experiencia y los informes presentados por muchos de las personas integrantes del foro gíreles presento esta tabla que recoge algunas de las características que deben ser tenidas en cuenta a la hora de la elección de las mismas para la auditoria wireless. No se pondrá bajo ningún concepto ningún precio ni ninguna dirección donde poder adquirirlas ya que estos datos cambian constantemente y será estudio particular de cada persona en función de sus necesidades y de su economía.

TABLA 1.2: TABLA DE TARJETAS INALÁMBRICAS (ACTUALIZADO A (3-10-06)
FUENTE: HTTP://WWW.SYMBOL.COM.MX/INFO8.HTML

Modelo	Chipset	Win	Lin	Inyección	Antena	Cobertura	Observaciones
AirisV257 mini-pci 11g	Ralink RT2500	No	Si	Lx (??)	No	Buena	Mini PCI
Belkin F5D7050	Ralink RT2570	No	Si	Lx (b/g)	No	Normal	Barata. USB, R. V3
CiscoAironet PCM352	Aironet	airo	Si	No+??	No	Buena	Necesario act. firmware
D-link DWL-510	RTL8180L	airo	Si	Lx (b/g)	Si	Normal	PCI. R A1. RTL = Realtek
Edimax EW-7128g	Ralink RT2500	No	Si	Lx (b/g)	Si	Normal	PCI
Gygabyte GN_WMAG	Atheros	airo	Si	Lx+??	No	**Muy sorda**	PCMCIA -108M
Intellinet 54 Wireless	Ralink RT2500	No	Si	Lx (b/g)	Si	**Sorda**	PCI.
IPW 2100 (Portatiles)	Intel Centrino	com	Si	No	No	Muy buena	Mini PCI. Cobertura OK
Linksys WMP54G v2	Broadcom	Si	??	No	No	**Sorda**	Difícil linux-drivers V2
Netgear WG311T (FS)	Atheros A2	**??**	Si	Lx(b/g)	Si	**Sorda**	Sicodelica
Orinco Gold 8470WD	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Normal	Pcmcia. Pigtail MC-Card
Senao2511cdplusext2	Prism 2.5	No	Si	Lx (b)	No	**Sorda**	Pcmcia. Pigtail MMCX
SMC SMCWPCIT-G	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Buena	PCI. Barata
Zcom XI-32HP+300W	Prism 2.5	No	Si	Lx (b)	Si	Normal	Pcmcia. Pigtail MMCX

1.4 Tendencia de Telecomunicaciones

1.4.1 Tecnología de las redes de telecomunicaciones

1.4.1.1 Wi – Fi

1.4.1.1.1 Definición e Historia

Wi-Fi (o Wi-fi, WiFi, Wifi, wifi) (del inglés Wireless Fidelity) es un conjunto de estándares para redes inalámbricas basados en las especificaciones 802.11. Creado para ser utilizado en redes locales inalámbricas; es frecuente que en la actualidad también se utilice para acceder a Internet. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance). El problema principal que pretende resolver la normalización es la compatibilidad. De esta forma en abril de 2000 WECA certifica la interoperatibilidad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi (Wíreless Fidelity, Fidelidad Inalámbrica).

Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps ya existen estándares que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por ese motivo, WECA anunció que empezaría a certificar también los equipos IEEE 802.11a de la banda de 5 Ghz mediante la marca Wi-Fi5. La norma IEEE.802.11 fue diseñada para sustituir a las capas físicas y MAC de la norma 802.3 (Ethernet).

1.4.1.1.2 Tipos de Wi - Fi

Hay tres tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. Un cuarto estándar, el 802.11n, está siendo elaborado y se espera su aprobación final para la segunda mitad del año 2007.

- Los estándares IEEE 802.11b e IEEE 802.11g disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Aunque estas velocidades de 108 Mbps son capaces de alcanzarse ya con el estándar 802.11g.

- En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además no existen otras tecnologías (Bluetooth, micro-ondas, etc.) que la estén utilizando, por lo tanto hay muy pocas interferencias.

La tecnología inalámbrica Bluetooth también funciona a una frecuencia de 2.4 GHz por lo que puede presentar interferencias con Wi-Fi, sin embargo, en la versión 1.2 y mayores del estándar Bluetooth se ha actualizado su especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías.

GRAFICO 1.9: TARJETA WI-FI PARA PALMONE
FUENTE: **DE WIKIPEDIA, LA ENCICLOPEDIA LIBRE**

1.4.1.1.3 Seguridad de Wi – Fi

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por

administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP y el WPA que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios. Actualmente existe el protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a WPA, es el mejor protocolo de seguridad para **Wi-Fi** en este momento.

1.4.1.1.4 Dispositivos para Wi - Fi

"Existen varios dispositivos que permiten interconectar elementos Wi-Fi, de forma que puedan interactuar entre si. Entre ellos destacan routers, puntos de acceso, para la emisión de la señal Wi-Fi y para la recepción se utilizan tarjetas para conectar a los PC, ya sean internas, como tarjetas PCI o bien USB (tarjetas de nueva generación que no requieren incluir ningún hardware dentro del ordenador). Los puntos de acceso funcionan a modo de emisor remoto, es decir, en lugares donde la señal wi-fi del router no tenga suficiente radio. Los router son los que reciben la señal de la línea que ofrezca el operador de telefonía, se encargan de todos los problemas inherentes a la recepción de la señal, donde se incluye el control de errores y extracción de la información, para que los diferentes niveles de red puedan trabajar. En este caso el router efectúa el reparto de la señal, de forma muy eficiente. Además de routers, hay otros dispositivos que pueden encargarse de la distribución de la señal, como pueden ser hubs y switch".[4]

1.4.1.2 WiMAX

1.4.1.2.1 Definición de WiMAX

[4] http://es.wikipedia.org/wiki/Wi-Fi

Una red combinada de Wi-Fi e implementación WiMAX, ofrece una solución más eficiente con base a costes que una implementación exclusiva de antena direccional de Wi-Fi o una malla de Wi-Fi se conecta con *backhaul* protegido con cable para abonados que quieren extender la red de área local o cubrir la última milla. Las redes Wi-Fi conducen la demanda para WiMAX aumentando la proliferación de acceso inalámbrico, aumentando la necesidad para soluciones del backhaul eficiente con base a costes y más rápida la última milla.

1.4.1.2.2 Características de WiMAX

- **Más alta productividad a rangos más distantes (hasta 50 km)**. Mejor bits/segundo/HZ en distancias largas.
- **Sistema escalable**. Fácil adición de canales maximiza las capacidades de las células.
- **Cobertura.** Soporte de mallas basadas en estándares y antenas inteligentes, permite mayor rango de alcance.
- **QoS (Quality of Service) Grant/Request MAC permite video y voz**. Servicios de nivel diferenciados.

1.4.1.2.3 Combinación Wi-Fi con WiMAX

La red ofrece un rango amplio de opciones inalámbricas de implementación para cubrir áreas grandes y de última milla. Lo mejor es que la solución varía de acuerdo a los modelos de uso, el tiempo de implementación, la posición geográfica y la aplicación de red (tanto en datos, VoIP y vídeo. Los Wi-Fi WLANs coexistirán con WiMAX. El IEEE 802.16 el estándar con revisiones específicas se ocupa de dos modelos de uso:

1.4.1.2.3.1 Fijo

“El estándar del 802.16-2004 del IEEE (el cuál revisa y reemplaza versiones del IEEE del 802.16a y 802.16d) es diseñado para el acceso fijo que el uso modela. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo parecido a un plato de la televisión del satélite. WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia”. [5]

1.4.1.2.3.2 Móvil

El estándar del 802.16e del IEEE es una revisión para la especificación base 802.16-2004 que apunta al mercado móvil añadiendo portabilidad y capacidad para clientes móviles con IEEE. Los adaptadores del 802.16e para conectarse directamente al WiMAX enlazan en red del estándar. El estándar del 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), lo cual es similar a OFDM en que divide en las subportadoras múltiples.

1.5 Redes Inalámbricas

1.5.1 Historia De Las Redes Inalámbricas

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal

[5] http://es.wikipedia.org/wiki/WiMAX

Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

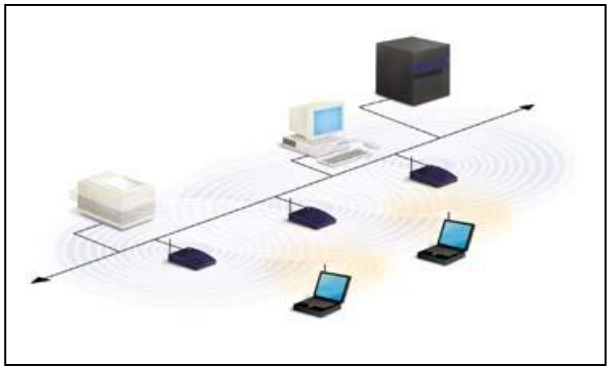
GRAFICO 1.10: REDES WLAN
FUENTE: WWW.AIRONET.COM

1.5.2 Definición De Redes Inalámbricas

Partamos de la definición de inalámbrico, este término se refiere al uso de la tecnología sin cables la cual permite la conexión de varios computadores entre sí. “Las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a

información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar. Con las WLANs la red, por si misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores".[6]

GRAFICO 1.11: REDES INALAMBRICAS
FUENTE: GRUPO INVESTIGADOR



1.5.3 Tipos De Tecnología Inalámbrica

1.5.3.1 Redes de área extensa (WAN)

La revolución más grande de la comunicación si cables se inició con los teléfonos móviles, los cuales han sido el producto electrónico con mayor éxito de todos lo tiempos. Inicialmente solo ofrecían comunicación por voz, ahora con baterías de mayor duración interfaces inteligentes, reconocimiento de voz y mayor velocidad, su uso futuro estará relacionado más con sus nuevos servicios inalámbricos.

1.5.3.2 Métodos de Acceso celular

[6] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 10-39

Los usuarios que ocupan un área geográfica deben disputarse un número limitado de canales y existen varios métodos de dividir el espectro para proporcionar acceso de forma organizada: El FDMA (Frequency División Múltiple Access), El TDMA (Time Division Multiple Access), El GSM (Global System for Mobile Communications), El CDAM (Code Division Multiple Access). Existen dos tipos principales de señales la analógica y la digital.

1.5.3.3 Redes de área local (LAN)

Una red de área local es un grupo de computadores y otros equipos relacionados que comparten una línea de comunicación y un servidor común dentro de un área geográfica determinada como un edificio de oficinas. Es normal que el servidor contenga las aplicaciones y controladores que cualquiera que se conecte a la LAN pueda utilizar.

1.5.3.4 Redes de área local sin cables (WLANs)

Ofrece acceso sin cables a todos los recursos y servicios de una red corporativa (LAN) en un edificio o todo un campus. Proporciona más libertad en el ambiente de trabajo. A través de una red sin cables los trabajadores pueden acceder a la información desde cualquierlugar de la compañía. Lo cual les ofrece numerosas ventajas:

- Acceso fácil y en tiempo real para realizar consultas desde cualquier lugar.
- Acceso mejorado a la base de datos.
- Configuración de red simplificada con mínima implicación MIS.
- Acceso independiente de la localización para administradores de redes.

1.5.3.5 Redes de área personal (PAN)

Existe dentro de un área relativamente pequeña, que conecta dispositivos electrónicos con ordenadores, impresoras, escáner, aparatos de fax, PDAs y ordenadores notebook, sin la necesidad de cables ni conectores para que sea efectivo el flujo de información. El

estándar de comunicaciones sin cables WPAN se centra en temas como el bajo consumo (para alargar la vida de los dispositivos portátiles), tamaño pequeño (para que sean más fáciles de llevar) y costos bajos (para que los productos puedan llegar a ser de uso masivo).

1.6. Estándares de Calidad de las Redes Inalámbricas

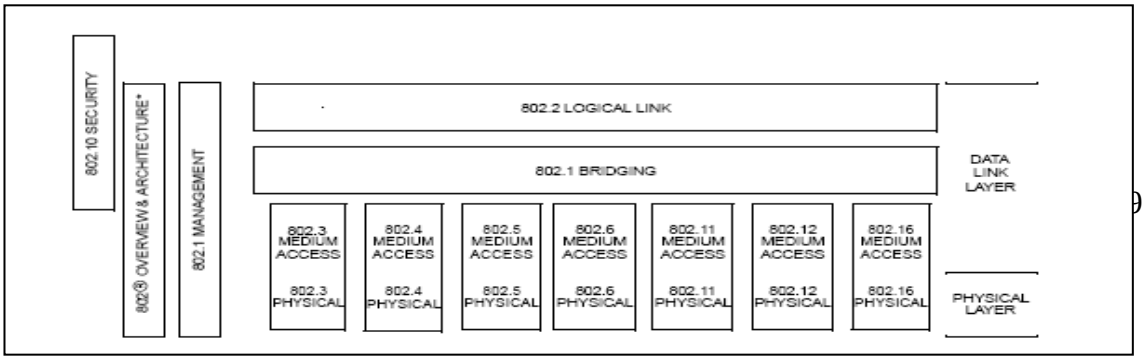
1.6.1 Estándar IEEE 802.11

Bajo el título de "Redes Wi-Fi", donde Wi-Fi proviene de Wireless Fidelity, agrupamos a un conjunto de redes de área local donde el medio de acceso es inalámbrico. Actualmente, las redes Wi-Fi están basadas en el conjunto de estándares IEEE 802.11 (IEEE: Institute of Electrical and Electronics Engineers).

1.6.2 Definición de los Estándares de la IEEE 802.11

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso de 802.11, tenemos extensiones 802.11a, 802.11b, etc. En realidad, el estándar 802.11 es sólo una parte de un conjunto más amplio de estándares de IEEE: el 802. La Figura muestra esquemáticamente la estructura del conjunto de estándares 802, dedicado a las capas más bajas de arquitectura de redes.

GRAFICO 1.12: FAMILIA DE LOS ESTANDARES DE LA IEEE. 802.11
FUENTE: GRUPO INVESTIGADOR



1.6.3 Características de las Tipologías de los Estándares de la IEEE 802.11

1.6.3.1 Estándar de la IEEE 802.11 b

Este estándar es una parte de una familia de los estándares para las redes del área local y metropolitana. Esta familia de los estándares con las capas de transmisión de la comprobación y de datos es de acuerdo a lo definido por el modelo de la referencia básica del Sistema Abierto de Interconexión de la Organización Internacional por Estandarización (ISO) (ISO/IEC 7498- 1:1994).

1.6.3.1.1 Descripción

Esta cláusula especifica la extensión de la alta tarifa del PHY para el sistema directo del espectro de la extensión de la secuencia (DSSS) (cláusula 15 del IEEE 802.11, en el año 1999, más luego se aplica como la alta tarifa PHY para la banda de 2.4 gigahertz señalada para los usos de ISM. Dicha extensión de las estructuras del sistema de DSSS en las capacidades de la tarifa de datos, según lo descrito en la cláusula 15 de IEEE 802.11, en el año 1999, para proporcionar 5.5 Mbit/s y 11 tarifas de datos de la carga útil de Mbit/s además del 1 Mbps y de 2 tarifas de Mbps. Para proporcionar las tarifas más altas, el código complementario 8-chip que afina (CCK) se emplea como el esquema de la modulación. La tarifa que salta es 11 megaciclos, que es igual que el sistema de DSSS descrito en la cláusula 15 de IEEE 802.11, del año 1999, así proporcionando la misma anchura de banda ocupada del canal. La nueva capacidad básica descrita en esta cláusula se llama el espectro directo de la extensión de la secuencia de la alta tarifa (hora DSSS). La alta tarifa básica PHY utiliza el mismo preámbulo y el jefe de PLCP que el DSSS PHY, así que PHYs puede coexistir en el

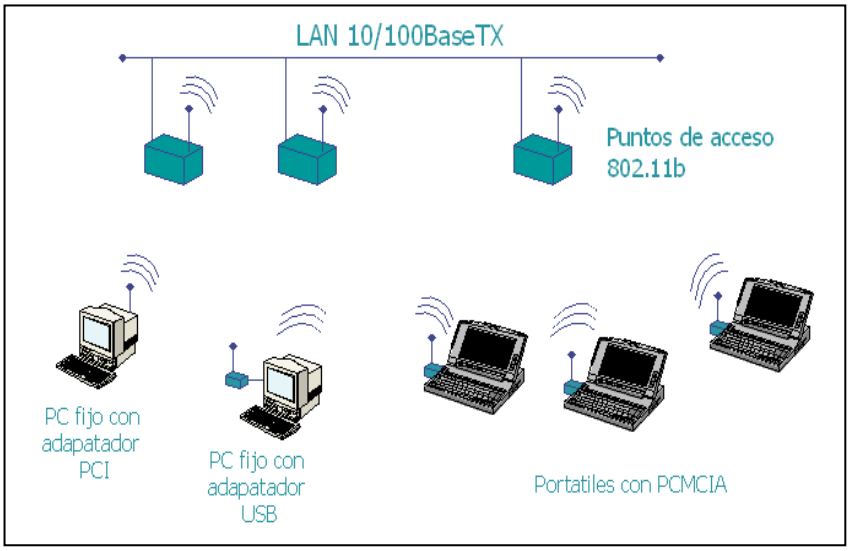
mismo BSS y puede utilizar el mecanismo de la conmutación de la tarifa en la manera prevista.

1.6.3.2 Estándar de la IEEE 802.11 g

IEEE y 802.11g, son marcas de fábrica registradas en los EE.UU. Por el Instituto de Eléctricos y Ingenieros Electrónicos. Cada padrón de IEEE es sujeto a la evaluación por lo menos cada cinco años, para la revisión o la reafirmación. Los documentos de niveles de IEEE son desarrollados dentro de las sociedades de IEEE, y los padrones coordinadas por el comité de Estándar, sus padrones a través de un proceso de consenso, y aprobadas por el Instituto Estadounidense de Estándares Nacionales. La existencia de un padrón de IEEE no insinúa que no hay ninguna otra manera de producir, hacer pruebas, medir, comprar el mercado, o proveer otros bienes y servicios relacionados con el alcance del padrón. Esta enmienda es parte de una familia de padrones para junta local y redes de área metropolitana, en la cual se arregla con el reconocimiento físico, a las capas de enlace de datos. "La organización para interconexión (OSI) modelo de referencia básico de sistemas abiertos de normalización (ISO) (ISO/IEC 7498, los padrones se definen en algunos tipos de tecnologías de acceso mediano, y son asociados a medios de comunicación físicos, apropiados para las aplicaciones especiales a los objetivos del sistema. Tiene un alcance de un Ancho de banda máximo de hasta 54 Mbps, Opera en el espectro de 2.4 Ghz sin necesidad de licencia, resulta ser compatible con el IEEE 802.11b, su Modulación es DSSS y OFDM".[7]

[7]"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.

GRAFICO 1.13: ESTANDARES DE CALIDAD PARA LAS REDES INALAMBRICAS
FUENTE: GRUPO INVESTIGADOR



1.6.3.3 Estándar de la IEEE 802.11 a

"El IEEE ratificó en julio de 1999 el estándar en 802.11a (los productos comerciales comienzan a aparecer a mediados del 2002), que con una modulación QAM-64 y la codificación OFDM (Orthogonal Frequency Division Multiplexing) alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros".[8]

1.6.3.4 Estándar de la IEEE 802.11 d

Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

[8] Hills. "Large-Scale Wireless LAN Design". IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

1.6.3.5 Estándar de la IEEE 802.11 e

El objetivo de dicho estándar es la mejora del nivel MAC del 802.11 para el aumento y la gestión de la QoS (Quality of Service), proporcionar una serie de servicios y mejorar el mecanismo de seguridad y autentificación. El objeto es permitir una gestión más eficaz de la banda en presencia de aplicaciones multimedia (voz, imagen y sonido).

1.6.3.6 Estándar de la IEEE 802.11 f

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio.

1.6.3.7 Estándar de la IEEE 802.11 h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélite.

1.6.3.8 Estándar de la IEEE 802.11 i

Se refiere al objetivo más frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11 Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de cifrado y procedimientos de autentificación. IEEE 802.1x constituye una parte clave de 802.11i.

1.6.3.9 Estándar de la IEEE 802.11 n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps, y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g.

1.7. Seguridad en las redes Inalámbricas de acuerdo a los Estándares

1.7.1 Definición

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

"Para que un intruso se pueda meter un nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar nuestra transmisión. Vamos a dar unos pequeños consejos para poder estar más tranquilos con nuestra red inalámbrica. Todos estos puntos son consejos, las redes inalámbricas están en pleno expansión y se pueden añadir ideas nuevas sobre una mejora de nuestra seguridad".[9]

1.7.1.1 *Medidas de Seguridad*

- Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.
- Control de acceso seguro con autentificación bidireccional.
- Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.

[9]http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml.

- Configuración WEP (muy importante) , la seguridad del cifrado de paquetes que se transmiten es fundamental en la redes inalámbricas, la codificación puede ser mas o menos segura dependiendo del tamaño de la clave creada y su nivel , la mas recomendable es de 128 Bits.
- Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.
- Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.
- Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

1.8. Vulnerabilidades

1.8.1 Deficiencias en la Encriptación Wep

El protocolo 802.11 implementa **encriptación WEP**, pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra red. Más que hablar de **la gran regla de la seguridad** podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

1.8.2 Después De Wep

WPA (Wi-Fi Protected Access), estándar desarrollado por la Wi-Fi alliance (WECA), que trata de ser el sustituto de WEP y es posible incorporarlo en algunos routers que no lo incorporan con una simple actualización de firmware. Esta está basada en los estándares IEEE 802.11i que mejoran de manera notoria la protección de datos y control de acceso, pudiendo decirse que el nivel de protección es alto ya que mejora el cifrado de datos mediante TKIP (Temporal Key Integrity Protocol) mediante claves de sesión dinámica por usuario, sesión y paquete, pero es necesario acceder a través de un server de autentificación y que asegura la confidencialidad de datos. Y por otro lado, WPA también ofrece la autentificación de los usuarios mediante el estándar 802.11x y EAP (Extensible Aunthentication Protocol) que permite controlar a todos y cada uno de los usuarios que se conectan a la red, aunque también permite, si se quiere, el acceso al usuario anónimo.

1.8.3 Ataques

1.8.3.1 Ataques A Las Redes Inalámbricas WLAN

Veamos un poco los diferentes tipos de ataques a redes inalámbricas y como funcionan. Para comenzar, vamos a dividir los ataques en activos y pasivos. Otros autores también definen más tipos de ataques, pero par ser mas prácticos, vamos a trabajar con estos dos. El siguiente listado menciona algunos de los ataques más comunes:

1.8.3.1.1 Ataques Activos.

Los ataques activos buscan causar algún daño, como ser: perdida de confidencialidad, disponibilidad e integridad de información ó sistemas.

- **IP Spoofing:** El atacante cambia su dirección IP para poder pasar por alto controles de acceso.

- **MAC Address Spoofing:** El atacante cambia su dirección MAC para pasar por alto los controles de acceso de los Access Points. Como veremos mas adelante, la mayoría de los Access Points posee controles de acceso filtrando direcciones MAC.

- **ARP Poisoning:** Todos los equipos conectados a una red tienen una tabla ARP que asocia direcciones MAC a direcciones IP. Este tipo de ataque busca modificar estas tablas para poder redirigir el tráfico de un equipo a otro de manera controlada.

- **Man in the middle:** Este tipo de ataque se puede ejecutar una vez realizado un ARP Poisoning, en el cual se redirige todo el trafico saliente de un equipo (victima) a otro y este lo envía al destino original. Este tipo de ataque es transparente y la victima no se da cuenta que su trafico de red esta pasando por un tercero antes de llegar a destino.

- **MAC Flooding:** Este ataque se consiste en inundar la red con direcciones IP falsas, causando que el Switch pase a funcionar en modo de Hub, ya que no soporta tanto tráfico.

- **Denial of Service:** Este tipo de ataque busca dejar fuera de servicio a la red inalámbrica, utilizando todo el ancho de banda para enviar paquetes basura. También se utiliza normalmente para dejar fuera de servicio a servidores ó aplicaciones.

- **Injection:** El atacante puede insertar paquetes en la red inalámbrica causando que todos los clientes se desconecten ó inundar la red con paquetes basura (generando un DoS).
- **Replay:** El atacante captura paquetes y luego los reinserta en la red inalámbrica con o sin modificación.

- **Rouge AP:** El atacante pone su propio Access Point y engaña a los clientes pensando que es el Access Point verdadero. De esta forma, posee todo el control del tráfico.

1.8.3.1.2 Ataques Pasivos.

Los ataques pasivos, en cambio, son aquellos donde un tercero no realiza ningún ataque, simplemente escucha.

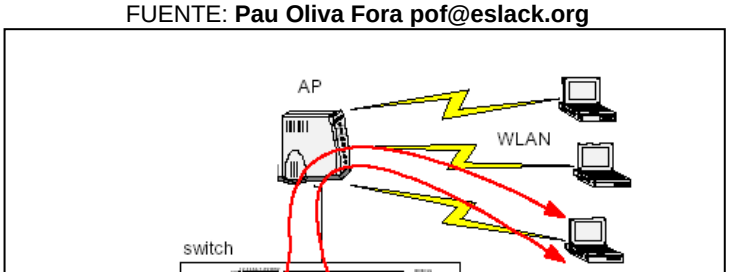
- **Eavesdropping:** El atacante simplemente escucha (generalmente con una notebook ó PDA) las comunicaciones entre un Access Point y sus clientes. Con este ataque se busca obtener información que es normalmente transmitida por la red, como ser: usuarios, contraseñas, direcciones IP, etc. Este tipo de ataque es el más peligroso, ya que abre las puertas a otros ataques.

Como hemos visto, los ataques son variados y todos pueden causar severos daños. En la siguiente sección, llamada "Anatomía de un ataque" demostraremos lo insegura que puede llegar a ser la tecnología inalámbrica para lo cual planteamos implementar seguridades en la red inalámbrica.

1.8.3.1.3 Ataque de Denegación de Servicio (DoS)

Para realizar este ataque basta con esnifar durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez que conoce su MAC, actúa como a nivel del AP. Lo único que tiene que hacer para denegar el servicio a un cliente es mandarle continuamente notificaciones (*management frames*) de desasociación. Si en lugar de a un solo cliente denegar el servicio a todos los clientes de la WLAN, mandando estas tramas a la dirección MAC de broadcast. Existen varias herramientas para realizar este ataque, las más comunes para el sistema operativo Linux son: **wlan-jack, dassoc.**

GRAFICO 1.14: LA COMUNICACIÓN DESPUES DEL ATAQUE
FUENTE: **Pau Oliva Fora pof@eslack.org**



1.9. Criterios y Comentarios de varios Autores sobre redes Inalámbricas y Seguridades en la misma

Según **MOREIRA** (Abril 2002)**,** define **REDES INALAMBRICAS** como: "Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos." (Pág. 21 - 26).

De acuerdo a lo expuesto por el autor consideramos que, **REDES INALAMBRICAS** es un conjunto de ordenadores que mantiene una estricta relación entre si a través de ondas electromagnéticas, que permitirá mantener una comunicación eficaz entre usuarios;

facilitando la operación en lugares donde la computadora no puede permanecer en un solo lugar.

Según **PERKINS** (Marzo 2003), **SEGURIDADES EN LAS REDES INALAMBRICAS** son**:** "Aquellas normas IEEE 802.11 que fueron diseñadas para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles."

De acuerdo con el autor nosotros creemos que, **SEGURIDADES EN LAS REDES INALAMBRICAS** son normas que permite corregir errores en el flujo de la información que circula a través de la red permitiendo de esta manera encontrar los errores y corregirlos; por lo tanto se hace necesario la implementación de seguridades en la red para el beneficio de la Universidad Técnica de Cotopaxi.

Según **VLADIMIROV** (Octubre 2006), **SEGURIDADES EN LAS REDES INALAMBRICAS** es**:** El motivo de la amplia cobertura de zonas de las redes 802.11 como uno de los motivos para tener presente un constante interés y preocupación por la seguridad, debido a que un atacante puede encontrarse en una zona donde nadie se lo espere encontrárselo y mantenerse suficientemente lejos del área física de la red, y aun estando protegidas con alguna tecnología como es WEP no están suficientemente protegidas por lo cual se recomienda implementar algún otro tipo de tecnología como WPA.

CAPITULO II

2. TRABAJO DE CAMPO: ELEMENTOS NECESARIOS PARA LA CONFIGURACION Y FUNCIONAMIENTO DE SEGURIDADES BAJO LOS ESTANDARES DE LA IEEE 802.11

2.1 Introducción

Hasta ahora sabemos dos cosas: nos gusta la tecnología Wi-Fi y sabemos que hay una norma (la 802.11) que la regula ¿Pero como funciona? Primero entendamos como funciona la tecnología inalámbrica. La norma 802.11 esta basada en la misma tecnología que hace funcionar nuestros teléfonos celulares. Toda la red inalámbrica se encuentra dividida en celdas. Cada una de estas celdas (llamadas según la norma 802.11 Basic Servicie Set ó BSS) esta controlada por una base ó Access Point. En el caso en que el radio de la celda no sea lo suficientemente grande como para abastecer el área que se requiere, es posible agregar más celdas.

La norma IEEE 802.11 fue diseñada para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles.

En el caso de las redes locales inalámbricas, está clara la cada vez mayor imposición del sistema normalizado por IEEE con el nombre 802.11g , norma conocida como Wi-Fi o Wireless Fidelity, aprobada en 1.990 y basada en el modelo OSI (Open System Interconnection), la primera norma 802.11 utilizaba infrarrojos como medio de transmisión para pasar hoy en día al uso de radiofrecuencia en la banda de 2.4 Ghz, con este sistema podemos establecer redes a velocidades que pueden alcanzar desde los 11 Mbps hasta los 54 Mbps estándares en los equipos actuales, aunque es posible alcanzar mayores velocidades. El estándar IEEE 802.11g alcanza velocidades más altas y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda

de frecuencia de 2,4 GHz y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.

Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El borrador del estándar también especifica tipos de modulación opcionales (como OFDM/CCK) diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.

2.1.1 Funcionamiento del Access Point

"Normalmente se pueden utilizar Access Point como repetidores de señal ó simplemente conectar uno más a la red de distribución (llamado Distribution System ó DS) y anexar otra celda a la primera. La red de distribución es simplemente una red existente (con cables ó fibra óptica), que brinda conectividad a los Access Point". [10]

Las 2 celdas, sus respectivos Access Point y la red de distribución son vistos como una única red, llamada según la norma 802.11 Extended Service Set ó ESS. El ESS debe tener un nombre ó identificación llamado SSID (Service Set Identifier) también conocido como "el nombre de la red". La figura 2.1 muestra una red inalámbrica con sus respectivos BSS, ESS y DS funcionando.

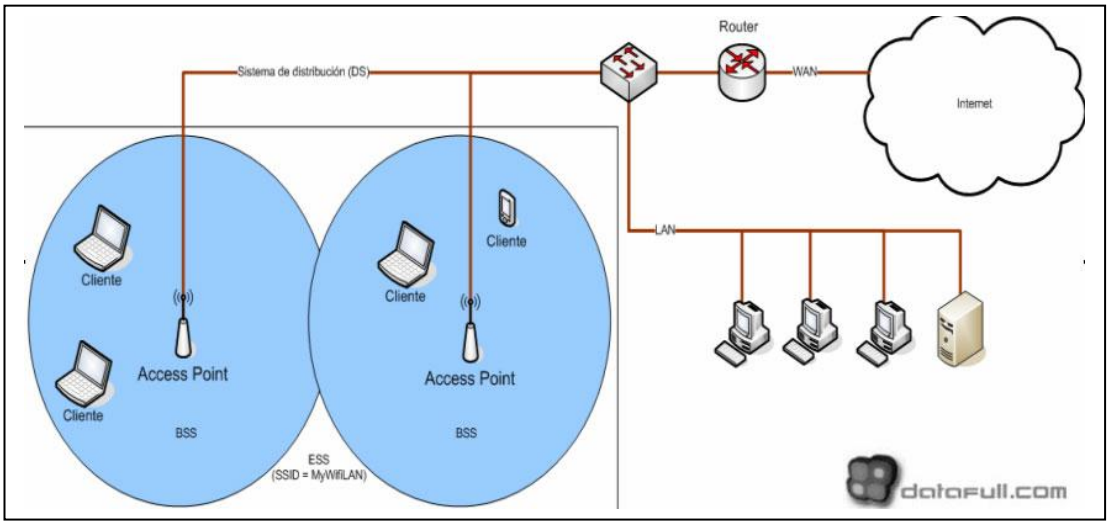
[10] http://www.pucelawireless.net/index.php?pagename=AccessPoint

Como se conecta un cliente a una red inalámbrica cuando una PC ó notebook (desde ahora cliente) se quiere conectar a una red inalámbrica, el hardware requiere cierta información del Access Point, como ser, la información de Sincronización. Esto puede obtenerse:

- De forma pasiva, en la cual el cliente espera que le llegue una transmisión del Access Point llamada Beacon Frame.
- De forma activa, en la cual el cliente envía una transmisión llamada Probe Request Frame y espera una respuesta para encontrar un Access Point.

Una vez que el Cliente encontró un Access Point y decide unirse a un BSS, comienza el proceso de autentificación. Por proceso de autentificación nos referimos a la forma en que el cliente se identifica (quien soy) y autentifica (probar que soy el que digo que soy) con el Access Point y así poder ingresar a la red inalámbrica.

GRAFICO 2.1: FUNCIONAMIENTO DEL ACCES POINT
FUENTE: GRUPO INVESTIGADOR



2.1.2 Antenas Seguras

Entre los modelos y variantes de antenas, se pueden distinguir 2 grandes familias: Las antenas Direccionales y las antenas Omnidireccionales.

2.1.2.1 Antenas Direccionales

Como su nombre indica, las direccionales emiten la señal hacia un punto en concreto, con mayor o menor precisión. Dentro del grupo de antenas direccionales, tenemos las de Rejilla o Grid, las Yagi, las parabólicas, las "Pringles" las de Panel y las Sectoriales.

2.1.2.2 Antenas Omnidireccionales

Las "Omni" por el contrario, emiten por igual en todas direcciones, en un radio de 360, pero solo sobre el plano perpendicular de la antena. Las omnidireccionales suelen ser una simple varilla vertical, aunque también tienen su tela. Hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias podremos cubrir con una antena, y con mejor calidad podremos captar señales que pudieran llegarnos muy débilmente. Algunas distancias conseguidas con antenas:

- Antena de Parrilla de 24dB de ganancia: 70,5 Km.
- Antena de Parrilla de 19dB de ganancia: 54 Km. entre dos antenas iguales.
- Antena Omnidireccional de 8dB de ganancia: 25 Km. de distancia, al otro extremo una de 19dB gris a 10km el enlace es 11Mbps, y a esa misma distancia conectamos entre 2 Omnis a 2Mbps.

2.1.2.3 El Pigtail:

No es más que un pequeño cable, que sirve de adaptación entre la tarjeta WIFI (o el AP) y la antena o el cable que vaya hacia la antena. Este Pigtail tiene 2 conectores: el propietario de cada tarjeta en un extremo, y por el otro un conector N estándar en la mayoría de los casos.

Antiguamente el pigtail era muy específico de cada producto, pero la situación se ha estabilizado y generalmente los conectores más habituales son los RSMA, RTNC, Lucent MC y MMCX.

2.1.2.4 Los modos de funcionamiento.

Tanto las tarjetas como los AP tienen diversas formas de trabajar, las más conocidas son AD-HOC e Infraestructura (Manager).

2.1.2.4.1 AD-HOC:

Una red "Ad Hoc" consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo de-igual-a-igual. Los ordenadores de la red inalámbrica que quieren comunicarse entre ellos necesitan configurar el mismo canal y ESSID en modo "Ad Hoc". La ventaja de este modo es que se puede levantar una comunicación de forma inmediata entre ordenadores, aunque su velocidad generalmente no supera los 11Mbps aunque su tarjeta soporte 125Mbps.

¿Qué es el ESSID?

Es un identificador de red inalámbrica. Es algo así como el nombre de la red, pero a nivel WIFI.

2.1.2.4.2. Infraestructura o Managed:

Esta es la forma de trabajar de los puntos de acceso. Si queremos conectar nuestra tarjeta a uno de ellos, debemos configurar nuestra tarjeta en este modo de trabajo. Solo decir que esta forma de funcionamiento es bastante más eficaz que AD-HOC, en las que los paquetes "se lanzan al aire, con la esperanza de que lleguen al destino.", mientras que la Infraestructura gestiona y se encarga de llevar cada paquete a su sitio. Se nota además el incremento de velocidad con respecto a AD HOC.

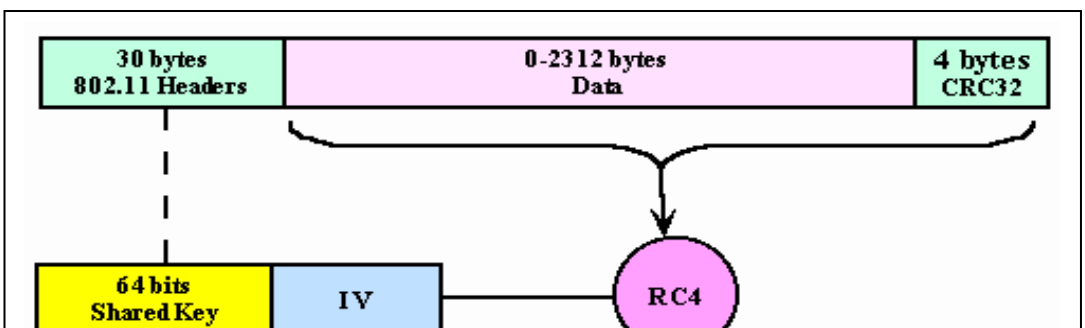
2.1.3 Encriptación Wep

Se puede habilitar o deshabilitar WEP y especificar una clave de encriptación. Wired Equivalent Privacy (WEP) proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado. Simplemente recordar que este método de seguridad NO ES VÁLIDO si realmente quieres proteger la red de accesos no autorizados. Una clave WEP puede romperse en pocos minutos, sin necesidad de conocimientos avanzados de informática.

2.1.3.1 El algoritmo de encriptación de WEP

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

GRAFICO 2.2: ALGORITMO DE ENCRIPTACION WEP
FUENTE: HTTP://WWW.MONOGRAFIAS.COM/TRABAJOS18/PROTOCOLO-WEP/PROTOCOLO-WEP.

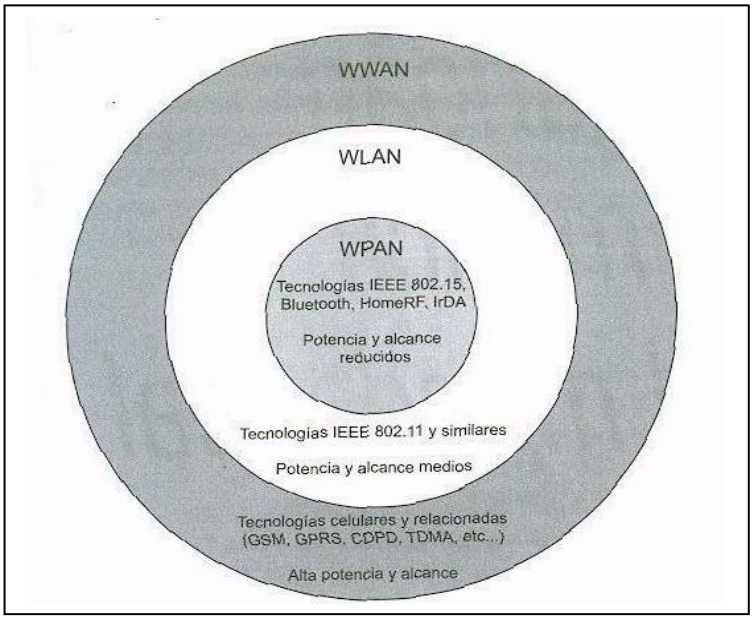


2.2 Seguridad Inalámbrica en el Mundo Real

En lugar de dedicarse a los conceptos básicos de seguridad de la información en general o de las redes inalámbricas. Este capitulo se encuentra en un punto en el cual muchos expertos suelen pasar por alto: el estado de seguridad inalámbrica en el mundo real. Antes de proseguir debemos tomar en cuenta tanto la seguridad de las redes inalámbricas basadas en estándares 802.11 y no en otro tipo de comunicación de radio de conmutación de paquetes. La figura muestra someramente las redes inalámbricas en la realidad, con las redes 802.11ocupando la franja intermedia.

Como podrá comprobar, tendemos a utilizar el término red inalámbrica 802.11 en lugar de LAN 802.11. Esta tecnología en particular desdibuja en el limite entre la conectividad de área local y amplia: los enlaces802.11 b punto a punto pueden llegar a mas de 80 Kilómetros de distancia, convirtiéndose de un modo eficaz en conexiones inalámbricas de una red WAN (red de área amplia) cuando se utiliza como solución de transporte para el ultimo par de kilómetros por parte de proveedores de servicios inalámbricos o como enlaces de largo alcance entre distintas oficinas. Por eso, consideramos necesario especificar el uso concreto de la tecnología 802.11: las redes LAN y WAN siempre tendrán distintas necesidades y enfoques sobre seguridad.

GRAFICO 2.3: VISTA GENERAL DE LAS REDES INALAMBRICAS MODERNAS.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



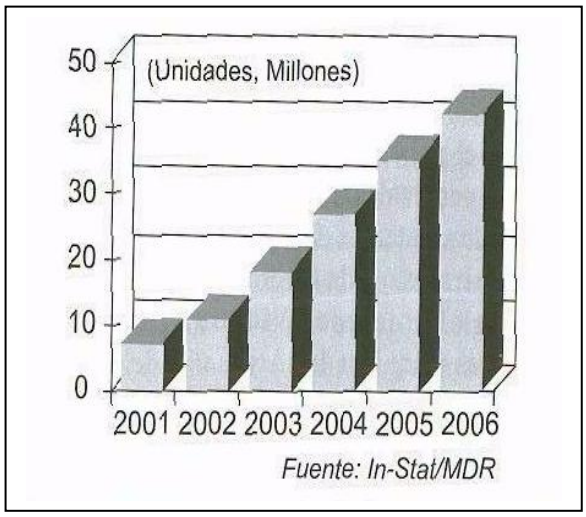
2.2.1 ¿Por que nos fijamos en la seguridad de los protocolos 802.11?

La amplia cobertura de zonas de las redes 802.11 es uno de los principales motivos para tener presente una constante preocupación e interés por la seguridad. Un atacante puede ubicarse en un lugar en que nadie espere encontrarlo y mantenerse suficientemente lejos del área física de la red. Otro motivo es el extenso uso de las propias redes 802.11: Se estima que en este año el numero de dispositivos de hardware con capacidades 802.11sobrepasarà las cuarenta millones de unidades, sobre todo a medida que el apareció de estas unidades vaya rebajándose. Después de que los productos 802..11g llegaran al mercado, el precio de muchas tarjetas de cliente 802.11b bajo hasta el nivel de precios de las tarjetas de red Ethernet 100BaseT.

Las redes 802.11 son omnipresentes, fáciles de encontrar y, como comprobará en esta explicación, a menudo no requieren ningún esfuerzo para conectarse con ellas. Incluso

aunque estén protegidas mediante WEP (que siga siendo una de las contramedidas de seguridad mas habituales en las redes 802.11), las debilidades del protocolo WEP han sido muy explicadas y son conocidas por prácticamente cualquier persona con un mínimo interés en las redes inalámbricas.

GRAFICO 2.4: CRECIMIENTO DEL MERCADO DE DISPOSITIVOS INALAMBRICOS 802.11.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



"Por el contrario, otras redes inalámbricas de paquetes conmutados no son ni de lejos tan habituales, no tienen vulnerabilidades muy conocidas y anunciadas y para su explicación suele nesecitarse hardware propietario muy caro y de disponibilidad reducida. Al mismo tiempo, los crackers de redes 802.11 suelen gestionar sus propias redes inalámbricas y utilizar sus equipos tanto para sus actividades ilícitas como para el trabajo en red domestica y en su comunidad".[11]

Los ataques contra teléfonos GSM y GPRS tienen que ver principalmente con la clonación de uni9dades, lo que se sale del ámbito de hacking inalámbrico. En cuanto a las redes de área personal (PAN, personal área network, la situación con respecto al hacking es mucho mas interesante de explorar desde el punto de vista de la consultaría de seguridad de redes.

[11] Vladimirov Andrew A., Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, 2005. Pág. 34-42

Los ataques contra redes personales de infrarrojos son una forma de ataque muy oportunista que se basa en encontrarse en el lugar apropiado en el momento correcto (un cracker tendrá que encontrarse cerca del dispositivo atacado y dentro de un sector de 30 grados a partir de su puerto de infrarrojos).

Ya que la potencia de la radiación infrarroja esta limitada a solo 2 mW, es de esperar que la señal no llegue más allá de los 2 metros. Una excepción a estos limites de 30 grados y 2mW se da en el caso en el que se despliega un punto de acceso infrarrojo (por ejemplo, Compex iRE201) en una oficina o sala de conferencias. En esta situación, todo lo que necesita hacer un cracker para analizar el tráfico y conectarse con la PAN inalámbrica es conectarse en la misma habitación que el punto de acceso. No existe seguridad en la capa 2 (la de enlace) en las redes personales IrDA (Asociación de datos por infrarrojos) y, a menos que se implanten sistemas de autentificación o cifrado en las capas superiores, la red de infrarrojos queda abierta para cualquiera que desee aprovecharse de ella. Los clientes de Windows 2000 y XP se asocian automáticamente con otras máquinas IrDA y la pila del proyecto Linux-IrDA, proporciona una opción de descubrimiento de máquinas IrDA remotas (irattach -s) al igual que irdadump, que es una herramienta similar a tcpdump. Se a podido utilizar irdaping para bloquear máquinas Windows 2000 que no tuvieran instalados los parches necesarios antes del Service Pack 3. Si desea volcar la información de los paquetes IrDA de la capa 2 de Windows 2000, la interfaz de depuración de infrarrojos de IrCOMM2k (una versión de la pila de Linux-IrDA), realizara un buen trabajo. Sin embargo, no importa como de inseguras sean las redes de infrarrojos, su uso tan reducido y sus límites en cuanto al alcance físico implican rastrear datos transmitidos mediante la luz jamás serán tan popular como buscar datos transmitidos en las ondas de radiofrecuencia (RF).

Por ese motivo, el warnibbling (buscar paquetes en redes de corto alcance) o la búsqueda de redes Bluetooth se volverá mucho mas popular que buscar conexiones de infrarrojos y podrá llegar a competir en popularidad con el wardriving (buscar redes de largo alcance) en algún momento. Ya hay disponibles herramientas para el descubrimiento de redes Bluetooth como red @Stake y una interfaz de usuario gráfica

(GUI) apropiada para esta herramienta () como Bluesniff, de Ssmo. Group) que se puede conseguir y utilizar problemas.

Existen tres factores limitadores de la extensión del hacking de Bluetooth. El primero de ellos es el uso tan limitado aún de esta técnica aunque es probable que esta tendencia cambie en unos pocos años. Otros mediante este protocolo. Sin embargo, los dispositivos Bluetooth de capacidades y puntos de acceso pueden cubrir un área de metros de radio o aun más si utilizan antenas de alta ganancia. Este sirve para ataques remotos. El tercer factor limitado constituyen los mecanismos de seguridad que protegen las redes personales Bluetooth. Hasta el momento no hay ningún ataque conocido que pueda saltarse el cifrado de flujo E0 que se usa para cifrar los datos en las redes personales Bluetooth. Sin embargo, al tiempo que podrá determinar si este sistema propietario de cifrado soportara el principio de Kerckhoff y si la famosa revolución no autorizará repetirse.

2.2.1.1 Las redes 802.11 ampliamente abiertas que nos rodean

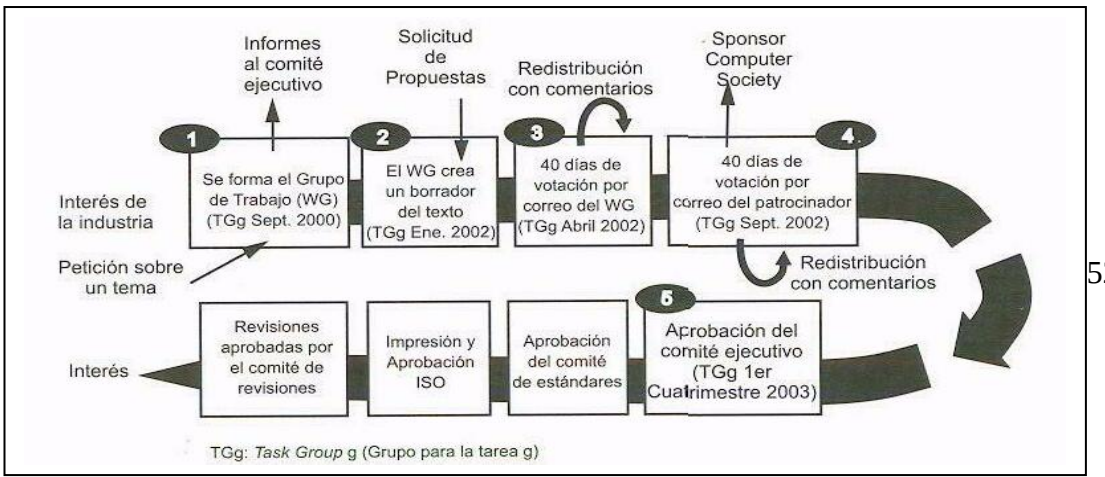
Como ya se ha comentado, en la mayoría de los casos un atacante no tiene que hacer nada en particular para conseguir lo que quiere. Se cree que la mayoría de las redes inalámbricas sin protección eran puntos de acceso de usuario domestico, redes de comunidades inalámbricas o de puntos de acceso publico, vuelve a estar equivocado. De hecho algunas corporaciones son importantes empresas del mundo de la tecnología de la información (IT) o consultoras relacionadas con el mismo, lo que resulta particularmente lamentable. Ni siquiera nos atrevemos a pensar en el número de las redes 802.11 localizadas que habían implantado medidas de seguridad apropiadas más allá de los estándares del protocolo WEP y el filtrado de direcciones MAC (fáciles de atacar).

2.2.1.2 El futuro de la seguridad 802.11

Los estándares 802.11 aliviaran esta situación de porvida, solo el tiempo lo dará la razón. Muchos fabricantes comenzaron a lanzar equipos 802.11 g al mercado, a pesar de que el estándar 802.11 no estaba completo. Una gran cantidad de estos productos previos al estándar 802.11 g se comunicaban como superseguros gracias al nuevo estándar. En realidad el estándar 802.11 g, en esencia se trata de la implementación del método de modulación de la capa física de 802.11 a mediante múltiplexación de división ortogonal de frecuencia (OFDM) para una banda ISM media (la banda no regulaba para uso industrial) con el objeto de proporcionar velocidad al estándar 802.11a (el máximo definido por el estándar es de 84 Mb/s), consiguiendo de este modo tanto una alta velocidad de conexión y compatibilidad con el estandar802.11 b o incluso con el espectro disperso de secuencia directa (DSSS) del estándar 802.11 original. Por ello, los intentos del mercado por enlazar el estándar 802.11 g con la seguridad.

Por otra parte, el estándar 802.11 i, es el nuevo estándar de seguridad inalámbrica destinado a sustituir al WEP y a proporcionar una seguridad inalámbrica mucho mas robusta, de acuerdo con sus desarrolladores. Se suponía que 802.11 i se haría publico junto con 802.11 g, pero no vivimos en un mundo perfecto. La versión 1 de la certificación WPA (Wireless Protected Access) de la Alliance implementa muchas de las características de desarrollo actual 802.11i, pero no todos los productos 802.11g actualmente en el mercado poseen certificación WPA, por el momento existen muchas redes 802.11 que siguen funcionando con versiones antiguas y inseguras del protocolo y hemos visto redes 802.11 g sin ningún tipo de cifrado de datos habilitado claramente debido a administradores poco consistentes de la seguridad.

GRAFICO 2.5: PROCESO DE DESARROLLO DEL PROTOCOLO 802.11 i.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.3 Autentificación de Usuario en la Seguridad Inalámbrica RADIUS

En esta sección describiremos los principios básicos de la metodología AAA, que se considera como la estructura fundamental detrás del servicio de Acceso Telefónico de Autentificación Remota (RADIUS).

2.3.1 Conceptos Básicos del Marco de Trabajo AAA

"La autentificación, autorización y administración de uso (AAA) puede interpretarse como una estructura para el control de acceso a recursos informáticos, la imposición de políticas, el análisis de uso de recursos y la obtención de la información necesaria".[12]

2.3.1.1 Autentificación

La autentificación es el proceso que proporciona un método para identificar a los usuarios mediante la petición y comparación de un conjunto válido de credenciales. La autentificación se basa en los criterios únicos que posee cada usuario para conseguir el acceso. El servidor conforme con AAA compara las referencias de autentificación del usuario con información almacenada en una base de datos. Si las credenciales se

[12] KONSTANTIN V, Hacking Wireless, GRUPO AMAYA S.A, Madrid, 2005. Pág. 390-401

corresponden, se le permite el acceso a los recursos de red solicitados; de no ser asì, el proceso de autentificación falla y se niega el acceso a la red.

2.3.1.2 Autorización

La autorización va después de la autentificación y es el proceso por el cual se determina si el usuario puede solicitar o utilizar ciertas tareas, recursos de red u operaciones. Normalmente la autorización se produce en el contexto de la autentificación y, una vez que se aprueba al usuario, este puede pasar a utilizar los recursos solicitados. Por ello, la autorización es un aspecto vital para la sana administración de una política de acceso.

2.3.1.3 Administración de Uso

El aspecto final de la estructura AAA es la contabilidad, que se describe mejor como el proceso de medida y grabación del consumo de los recursos de red. Este permite la monitorización y la generación de informes sobre eventos y su uso para distintos propósitos, incluidos la presentación de facturas, el análisis de tendencias, el uso de recursos, la planificación de capacidad y el mantenimiento activo de la política.

2.3.2 Vista General del Protocolo RADIUS

RADIUS es un protocolo muy utilizado que se implementa en muchos entornos de red. Puede definirse como un protocolote seguridad que emplea un enfoque cliente servidor para autentificar a los usuarios remotos. Esta seguridad se consigue mediante una serie de desafíos y respuestas que el cliente realiza entre el servidor de acceso a la red (el NAS) y el usuario final. El protocolo RADIUS se creo debido a la creciente necesidad de un método de autentificación, autorización y administración de uso para usuarios que necesitaban acceder a entornos informáticos heterogéneos.

2.3.3 Características de RADIUS

La RFC 2138 identifica las siguientes características clave del protocolo RADIUS.

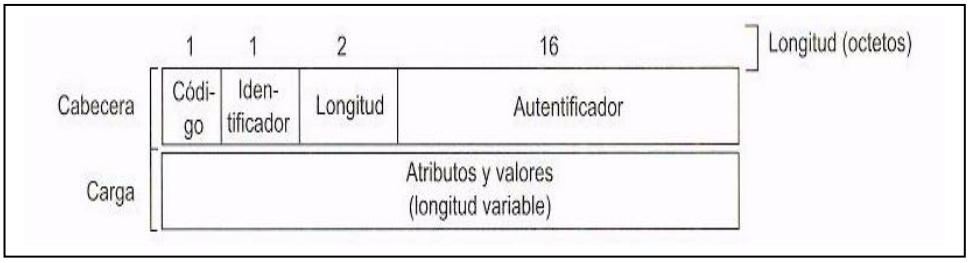
- **Modelo Cliente/ Servidor:** Un NAS funciona como un cliente de RADIUS. El cliente es el responsable de transferir la información de usuario a los servidores RADIUS designados y de actuar consecuentemente con la respuesta recibida. Los servidores RADIUS son los responsables de recibir las peticiones de conexión de los usuarios, de llevar a cabo la autentificación y de devolver continuación todos los detalles de configuración necesarios para que el cliente proporcione los servicios al usuario. Adicionalmente, el servidor RADIUS puede funcionar como cliente indeterminado hacia otros servidores RADIUS o servidores de autentificación similares.
- **Seguridad de red:** La comunicación entre el cliente y el servidor RADIUS se autentifica mediante el uso de una clave compartida que nunca se envía a través de la red como texto plano. Además, las contraseñas de usuario se envían cifradas entre el cliente y el servidor RADIUS, para eliminar la posibilidad de un ataque de escucha.
- **Mecanismos de autentificación flexibles:** El servidor RADIUS permite usar una amplia variedad de métodos para autentificar a un usuario. Cuando se le proporciona el nombre de usuario y la contraseña original utilizada por el usuario, puede soportar PAP o CHAP, el sistema de acceso de UNIX y otros métodos de autentificación como PAM, LDAP, SQL Y DEMÀS.
- **Protocolo Extensible:** Todas las transacciones constan de tuplas Atributo-Longitud-Valor (ALV) de longitud variable. Se pueden añadir atributos nuevos sin perturbar las implementaciones ya existentes del protocolo, con lo que el protocolo resulta más flexible y dinámico para soportar implementaciones nuevas.

2.3.4 Formato de Paquetes

El paquete de RADIUS se encapsula en un flujo de datos UDSP sin estado que se envía a los puertos de destino 1812 1813 y 1814, que representan respectivamente el acceso, la contabilidad y la intermediación. Por compatibilidad y mantener los valores históricos, algunos servidores siguen funcionando, erróneamente, sobre los puertos 1645 y 1676. Este comportamiento viene de las primeras etapas del desarrollo de RADIUS y en la actualidad entra en conflicto con el servicio de medición de datos (o datametrico).

La RFC especifica que RADIUS utiliza una etsuctura de paquete esperada para el proceso de comunicación, que muestra la figura.

GRAFICO 2.6: ESTRUCTURA DE UN PAQUETE DE RADIUS.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



A continuación describiremos los elementos del paquete RADIUS:

- **Código:** El campo código tiene una longitud de un octeto e identifica el tipo de paquete RADIUS. Cuando un servidor recibe un paquete con un campo de código no valido, lo ignora sin ningún tipo de notificación adicional.
- **Identificador:** El identificador es un valor de un octeto que permite al cliente RADIUS comparar una respuesta RADIUS con la petición pendiente correcta.
- **Autentificador:** Este valor tiene una longitud de 16 octetos y se utiliza para autentificar y verificar la respuesta procedente del servidor RADIUS. También

se utiliza como mecanismo de ocultación de contraseñas. Los dos tipos de valor son los autentificadotes de Petición y respuesta.

- **Atributos:** La sección de atributos del paquete clasifica diversas características y patronos de comportamiento de servicio, que suele anunciar una característica en particular del tipo de servicio ofrecido o solicitado.

TABLA 2.1: TIPOS DE ATRIBUTOS DE RADIUS.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.

Valor del atributo	**Longitud en octetos**	**Tamaño (en bits)**	**Ejemplos**
INT (entero)	4	32	256 65536
ENUM (enumerador)	4	32	1= nombre de usuario 2= contraseña de usuario 13=compresión de marco 26=especifico del fabricante
SRING (cadena)	1-253	Variable	“cualquier cadena” “192.168.111.111”
IPADDR (dirección IP)	4	32	0xFFFFFF 0x00000A
DATE (fecha)	4	32	0xFFFFFF 0x00000A
BINARY (binario)	1	1	0

2.3.5 Tipos de Paquetes

El servidor RADIUS identifica los tipos de mensajes de acuerdo con el campo Código del paquete RADIUS.

TABLA 2.2: CODIGOS DE PAQUETE DE RADIUS.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.

Código RADIUS	**Descripción**
1	Petición de Acceso
2	Aceptación de Acceso
3	Rechazo de Acceso
4	Petición de Contabilidad
5	Respuesta de Contabilidad
11	Desafió de Acceso
12	Estado del Servidor (experimental)
13	Estado del Cliente (experimental)
255	Reservado

2.4 Estándares de Calidad para el Aseguramiento del flujo de la Información de la red Inalámbrica bajo Estándares Internacionales

Para el presente trabajo investigativo nos hemos basado en algunos estándares que rigen las redes y las telecomunicaciones, de esta manera aseguramos un correcto estudio de la situación actual de la Universidad y podemos sugerir con certeza las mejoras que deben implementarse en la red corporativa de la Universidad Técnica de Cotopaxi.

Por su campo de acción se evaluó los siguientes estándares los mismos que damos a conocer a continuación.

2.5 Estándares de la IEEE 802.11b-1999

Este estándar es parte de una familia de los estándares 802.11para las redes inalámbricas del área local y metropolitana. La relación entre el estándar y otros miembros de la familia lo demostraremos a continuación en breves contenidos.

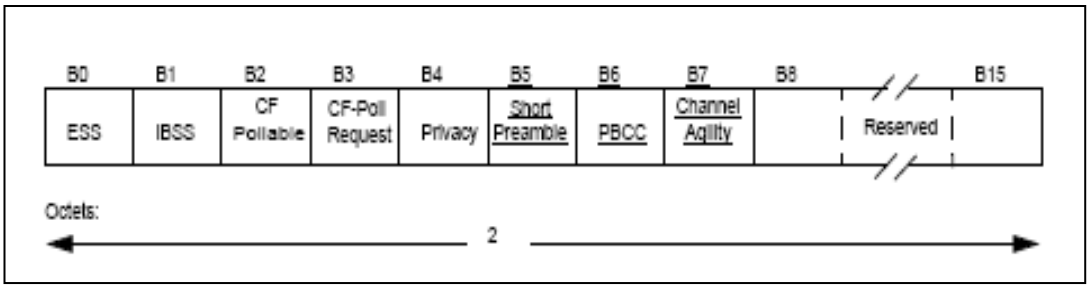
2.5.1. Sistema básico determinado de la tarifa del servicio básico (BSS)

El sistema de tarifas de transferencia de datos de todas las estaciones de un BSS será capaz de usar, recibir y transmitir los marcos desde la forma el medio sin hilos (WM). Las tarifas de datos determinadas de la tarifa básica de BSS se preestablecen para todas las estaciones en el BSS.

2.5.1.1 Campo de información de la capacidad

El campo de información de la capacidad contiene un número de subcampos que se utilizan para indicar capacidades solicitadas o anunciados. La longitud del campo de información de la capacidad es 2 octetos. El campo de información de la capacidad consiste en los subcampos siguientes: ESS, IBSS, CF-Pollable, petición de CF-Poll, y aislamiento, preámbulo corto, PBCC, y agilidad del canal. El formato del campo de información de la capacidad está según lo ilustrado en la figura.

GRAFICO 2.7: CAPACIDAD DEL CAMPO FIJO DE LA INFORMACIÓN
FUENTE: **Tomado del Estándar IEEE 802.11b-1999**



2.5.1.2 DCF

El protocolo del acceso medio permite que las estaciones apoyen diversos sistemas de tarifas de datos. Todo los STAs podrá recibir y transmitir datos en todas las tarifas y lo transmiten en uno o más Sistemas Básicos de las tarifas de datos. Para apoyar la operación apropiada del RTS/CTS y del portador virtual se necesita detectar el mecanismo, todo el STAs podrá detectar los marcos de RTS y de CTS. Por esta razón, los marcos de RTS y de CTS serán transmitidos en cada una de las tarifas determinadas del Sistema Básico de la tarifa básica de BSS.

5.2.1.3 Ayuda de Multitarea

Algún PHYs tiene capacidades múltiples de la tarifa de transferencia de datos que permitan que las puestas en práctica realicen la conmutación dinámica de la tarifa con el objetivo de mejorar funcionamiento. El algoritmo para realizar la conmutación de la tarifa está más allá del alcance de este estándar, pero para asegurar coexistencia e interoperabilidad en PHYs multitarea-capaz, este estándar define un sistema de las reglas que serán seguidas por todo el STAs. Todos los marcos del control serán transmitidos a una de las tarifas en el Sistema Básico de la tarifa de BSS.

2.5.1.3.1 Exploración Confirmada del MLME

El cambio "fijó" a los "sistemas" se lo demostrara en la tabla de las columnas del nombre y de la descripción para el sistema de parámetro de PHY.

TABLA 2.3: SEMÁNTICA DEL SISTEMA PRIMITIVO.
FUENTE: **Tomado del Estándar IEEE 802.11b-1999**

Nombre	**Tipo**	**Rango Valido**	**Descripción**
BSSID	**Dirección MAC**	N/A	El BSSID del BSS encontrado.
SSID	Secuencia del octeto	1–32 octetos	El SSID del BSS encontrado.
Tipo BSS	Enumeración	Infraestructura, Independiente	El tipo del BSS encontrado

Período Del Faro	Número entero	N/A	El período del faro del BSS encontrado (en TU).
Periodo DTIM	Número entero	Según lo definido en formato del marco	El período de DTIM del BSS (en períodos del faro).
Tiempo Local	Número entero	N/A	El valor del contador de tiempo de TSF del sTA en el comienzo de la recepción del primer octeto.
Sistema De Parámetro de PHY	Según lo definido en formato del marco	Según lo definido en formato del marco	El sistema de parámetro relevante al PHY
Sistema De Parámetro de los CF	Según lo definido en formato del marco	Según lo definido en formato del marco	El sistema de parámetro relevante al PHY
Sistema De Parámetro de IBSS	Según lo definido en formato del marco	Según lo definido en formato del marco	El sistema de parámetro para el IBSS, si BSS encontrado es un IBSS.
Información De la Capacidad	Según lo definido en formato del marco	Según lo definido en formato del marco	Las capacidades anunciadas del BSS.
Sistema De la Tarifa De BSSB Básica	Sistema de enteros	1-27 inclusive (para cada número entero en el sistema)	El sistema de las tarifas de datos (en las unidades de 500 kb/s) que se deben apoyar por todo el STAs que desee ensamblar este BSS. El STAs debe poder recibir y transmitir en cada uno de las tarifas de datos
Descripción BSS	Descripción BSS	N/A	La Descripción BSS es un miembro del sistema que fue vuelto como resultado de una

			petición de MLMESCAN.
Ensamble El Descanso De la Falta	Número entero	≥ 1	El límite de tiempo, en unidades de los intervalos del faro, después de lo cual el procedimiento del unido serán terminados.
La Punta de prueba Retrasa	Número entero	N/A	Ser utilizado antes de transmitir un marco de la punta de prueba durante la exploración activa.
Sistema Operacional De la Tarifa	Sistema de números enteros	inclusivo (para cada número entero en el sistema)	El sistema de las tarifas de datos (en las unidades de 500 kbit/s) que el STA desea utilizar para la comunicación dentro del BSS. El STA debe poder recibir en cada uno de las tarifas de datos enumeradas en el sistema.

2.5.2 Alta tarifa, especificación directa del espectro PHY de la extensión de la secuencia

2.5.2.1 Descripción.

Esta cláusula especifica la extensión de la alta tarifa del PHY para el sistema directo del espectro de la extensión de la secuencia (DSSS) (cláusula 15 del estándar IEEE 802.11, edición 1999), más conocido como la alta tarifa PHY para la banda de 2.4 gigahertz señalada para los usos de ISM.

“Esta extensión de las estructuras del sistema de DSSS se encuentra en las capacidades de la tarifa de datos, para proporcionar 5.5 Mbit/s y 11 tarifas de datos de la carga útil de

Mbit/s además del 1 Mbps y de 2 tarifas de Mbps. Para proporcionar las tarifas más altas, el código complementario 8-chip que afina (CCK) se emplea como el esquema de la modulación. La tarifa que salta es 11 megaciclos, que es igual que el sistema de DSSS, así proporcionando la misma anchura de banda ocupada del canal. La nueva capacidad básica descrita en esta cláusula se llama el espectro directo de la extensión de la secuencia de la alta tarifa (hora DSSS). La alta tarifa básica PHY utiliza el mismo preámbulo y el jefe de PLCP que el DSSS PHY, así que PHYs puede coexistir en el mismo BSS y puede utilizar el mecanismo de la conmutación de la tarifa en la manera prevista".[13]

2.5.2.2 Alcance.

Esta cláusula especifica la entidad de PHY para la extensión de HR/DSSS y los cambios que tienen que ser realizados al estándar de la base para acomodar la alta tarifa PHY.

La capa de la alta tarifa PHY consiste en las dos funciones siguientes del protocolo:

- Una función de la convergencia de PHY, que adapta las capacidades del sistema dependiente medio físico (PMD) al servicio de PHY. Esta función es apoyada por el procedimiento de la convergencia de PHY (PLCP), que define un método para trazar las unidades de datos de protocolo de la subcapa del MAC (MPDU) en un formato que enmarca conveniente para enviar y recibir datos del usuario y la información de la gerencia entre dos o más STAs usando el sistema asociado de PMD. El PHY intercambia las unidades de datos de protocolo de PHY (PPDU) que contienen las unidades de datos de servicio de PLCP (PSDU). El MAC utiliza el servicio de PHY, así que cada MPDU corresponde a un PSDU que se lleve adentro un PPDU.
- Un sistema de PMD, del las cuales función define las características, y método de transmitir y de recibir datos por, un medio sin hilos entre dos o más STAs, cada uno que usa el sistema de la alta tarifa PHY.

[13] Tomado del Estándar IEEE 802.11b-1999

2.5.2.3 Funciones de la alta tarifa PHY

La arquitectura de la alta tarifa PHY de 2.4 gigahertz se representa en el modelo de la referencia básica de ISO/IEC demostrado en el cuadro 137. La alta tarifa PHY contiene tres entidades funcionales: la función de PMD, la función de la convergencia de PHY, y la función de la gerencia de capa. El servicio de la alta tarifa PHY será proporcionado al MAC a través de los primitivos de servicio de PHY.

2.5.2.4 Subcapa de La Alta Tarifa PLCP

2.5.2.4.1 Descripción

Este subclase proporciona un procedimiento de la convergencia para la especificación de 2, 5.5, y 11 Mbit/s, en la cual PSDUs se convierte a y desde PPDUs. Durante la transmisión, el PSDU será añadido a un preámbulo y al jefe de PLCP para crear el PPDU. Se definen dos diversos preámbulos y jefes: el preámbulo y el jefe largos apoyados obligatorios, que ínter opera con la corriente 1 Mbit/s y 2 especificación de Mbit/s DSSS (según lo descrito en el Estándar IEEE 802.11, Ediciones 1999), un preámbulo y un jefe corto opcional. En el receptor, el preámbulo y el jefe de PLCP se procesan para ayudar en la desmodulación y la entrega del PSDU.

2.5.2.4.2 Formato de PPDU

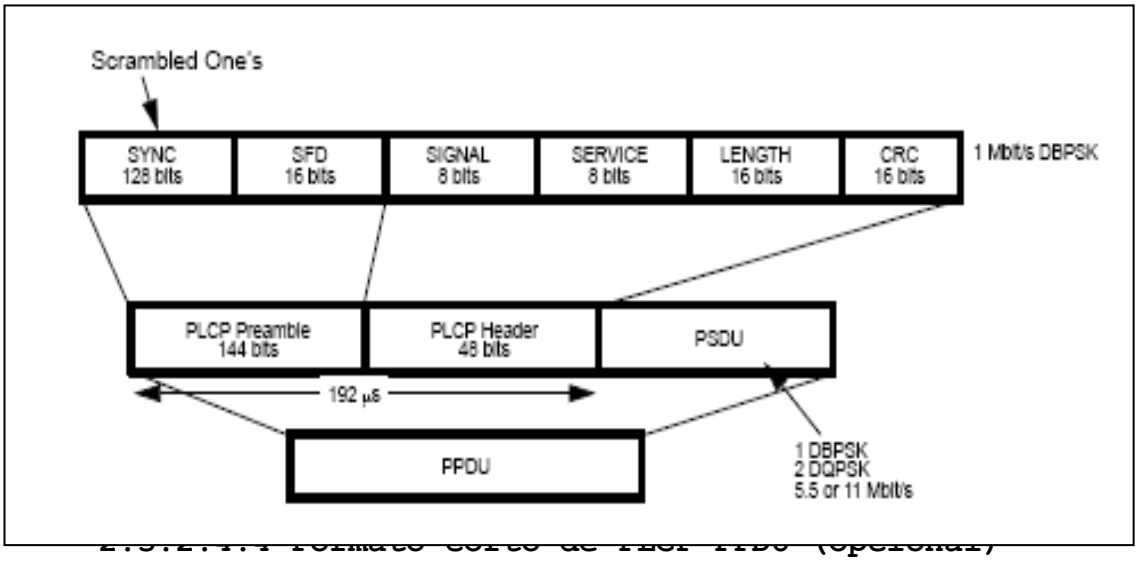
Se definen dos diversos preámbulos y jefes: especificación del preámbulo largo apoyado obligatorio y del jefe que es interoperable con la corriente 1 Mbit/s y 2 de Mbit/s DSSS (según lo descrito en Estándar IEEE 802.11, Ediciones 1999), un preámbulo y un jefe corto opcional.

2.5.2.4.3 Formato largo de PLCP PPDU

La figura demuestra el formato para el PPDU (largo) interoperable, incluyendo el preámbulo del alta tarifa PLCP, el jefe del alta tarifa PLCP, y el PSDU. El preámbulo de

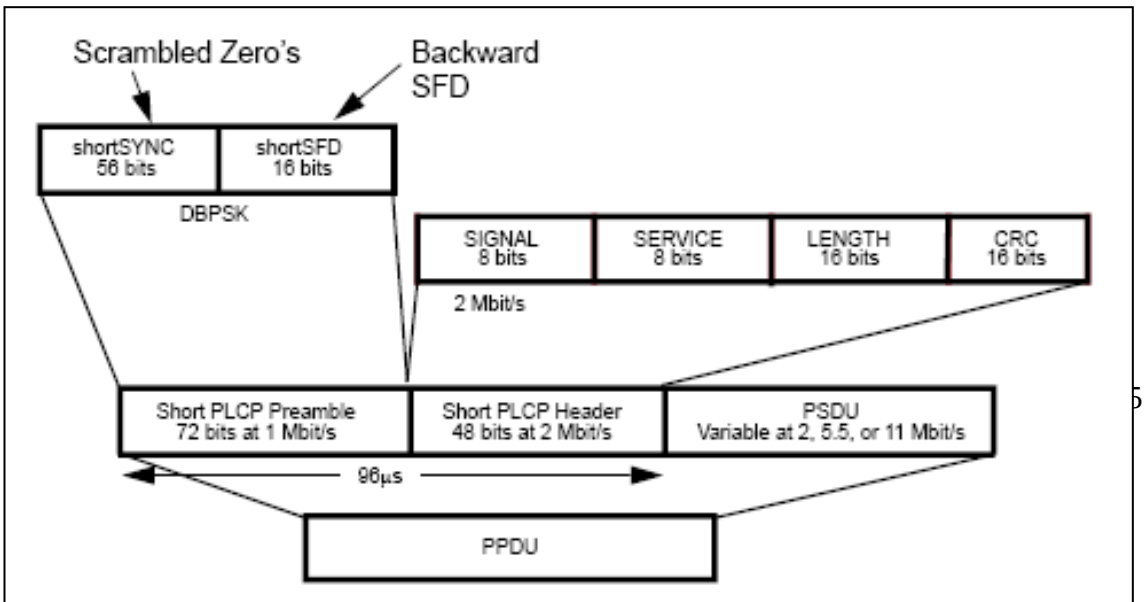
PLCP contiene los campos siguientes: sincronización (sinc.) y delimitador del marco del comienzo (SFD). El jefe de PLCP contiene los campos siguientes: el señalar (SEÑAL), servicio (SERVICIO), longitud (LONGITUD), y CCITT CRC-16.

GRAFICO 2.8: **FORMATO LARGO DE PLCP PPDU**
FUENTE: **Tomado del Estándar IEEE 802.11b-1999**



El preámbulo y el jefe cortos (HR/DSSS/short) de PLCP se define como opcionales. El preámbulo y el jefe cortos se pueden utilizar para reducir al mínimo gastos indirectos y, así, para maximizar el rendimiento de procesamiento de datos de la red. El formato del PPDU, con HR/DSSS/short, se representa en el cuadro.

GRAFICO 2.9: **FORMATO CORTO DE PLCP PPDU**
FUENTE: **Tomado del Estándar IEEE 802.11b-1999**



2.6 Estándares De La IEEE 802.11g-2003

2.6.1 Especificación de PHY de potencia

2.6.1.1 Visón General

Esta cláusula especifica que la extensión de potencia adicional del PHY para la secuencia de dirección lo difundió (DSSS). A partir de estas cláusulas el PHY definido en la misma será conocido como el PHY de potencia ampliado (ERP). Este PHY opera en la banda de ISM 2.4 gHz.

2.6.1.2 Introducción

El ERP desarrolla Mbit/s, DSSS se usa sobre las potencias de datos de carga útil de 1 y 2 Modulaciones y complexiones sobre las potencias de datos de carga útil de 1, 2, 5.5, y 11 Mbit/s, DSSS usa CCK, y las modulaciones de PBCC opcionales. El ERP se basa en

C para proveer adicionalmente. La capacidad por 1, 2, 5.5, 11, 6, 12, y 24 potencias de datos de Mbit/s es obligatoria. Dos ERP opcionales y adicionales usan los modos de modulación de PBCC con potencia de datos de carga útil de 22 y 33 Mbit / s.

2.6.1.3 Los modos de operaciones

La porción de radio de todas las cláusulas de los sistemas de ERP compatibles excepto algunas usa la frecuencia 2.4 gHz. Uno BSS de ERP es capaz de operar en cualquier combinación de modos de ERP disponibles ya sean (PHYs) y modos de ERP.

2.6.1.4 Funciones de PHY de potencias prolongadas

La arquitectura del ERP es retratada en el ISO/IEC modelo de referencia básica. El ERP contiene tres entidades funcionales: la función de PMD, la función de convergencia de PHY (PLCP), y la dirección de capa en la cual funciona. La interoperabilidad del mensajero de mecanismo de sentido y la protección, permite que centros de ERP oigan hablar del tráfico de ERP para de esta manera poder cumplir él propósito de que pueden diferir el medio a ese tráfico.

2.6.1.5 PHY - la lista de parámetro del servicio específico

La arquitectura del MAC de IEEE 802.11 es apropiada para ser PHY independiente, algunas puestas en práctica de PHY, como son la entidad de dirección (MLME), en cierto PMD con el que las puestas en práctica, el MLME pueden necesitar interactuar el PLME como parte de los primitivos de SAP de PHY normales. La lista definió a primitivos del servicio en el PHY actualmente como TXVECTOR y RXVECTOR. La lista de estos parámetros, y los valores que pueden representar son definidos en las especificaciones de PHY específicas para cada PMD:

- Algunos primitivos del servicio incluyen un vector de parámetro. DATARATE y la duración.
- Los parámetros son considerados ser los parámetros de dirección y son propios de este PHY.
- Los parámetros en la tabla son definidos como parte de la lista de parámetro de TXVECTOR en el PHYTXSTART.

TABLA 2.4: **PARÁMETROS DE TXVECTOR**.
FUENTE: **Tomado del Estándar IEEE 802.11g-2003**

PARAMETRO	VALOR
DATOS DE POTENCIA	La tarifa solía transmitir el PSDU en Mbit/s Admite que el valor depende del valor del parámetro de modulación: - ERP DSSS: 1 y 2 - ERP CCK: 5.5 y 11 - ERP OFDM: 6, 9, 12, 18, 24, 36, 48, y 54 - ERP PBCC: 5.5, 11, 22, y 33 DSSS - OFDM: 6, 9, 12, 18, 24, 36, 48, y 54.
LONGITUD	La longitud del PSDU en octetos alcance: 1 - 4095.
TIPO _ PREÁMBULO	El preámbulo se usa para la transmisión del PPDU Enumeró el tipo para el que el valor admitido depende del valor de la modulación Parámetro: ERP - OFDM: nulo ERP - DSSS, ERP - CCK, ERP - PBCC, DSSS - OFDM: SHORTPREAMBLE, LONGPREAMBLE.
MODULACIÓN	La modulación se usa para la transmisión de este PSDU

	Tipo enumerado: ERP - DSSS, ERP - CCK, ERP - OFDM, ERP - PBCC, DSSSOFDM.
SERVICIO	- El vector de inicialización de encriptador. - Cuando el formato de modulación seleccionado es ERP - OFDM o DSSS – OFDM. - Las partes nulas son usadas para la inicialización de encriptador. - Las partes son se reservadas. - Para todas las modulaciones de ERP que todos empiezan con ERP - DSSS breve o largo el preámbulo, los bits del campo del servicio son definidos en 123C de mesa y el campo del servicio no es aplicable en el TXVECTOR así que el campo entero lo es para reservar.
TXPWR_NIVEL	El transmitir el nivel a motor. La definición de estos niveles está involucrada en el implementar 1 - 8.

2.6.2 PLCP de potencia ampliado.

2.6.2.1 Introducción

Suministra un procedimiento de convergencia de capa de PHY (PLCP) para el ERP. El procedimiento de convergencia, especifica cómo son transformadoras y desde PPDUs en el transmisor y el auricular PSDUs. El PPDU durante la transmisión de datos añadiendo el PSDU al preámbulo de PLCP. En el auricular, el PLCP del que preámbulo y encabezamiento son procesados a la ayuda en la desmodulación y la entrega el PSDU.

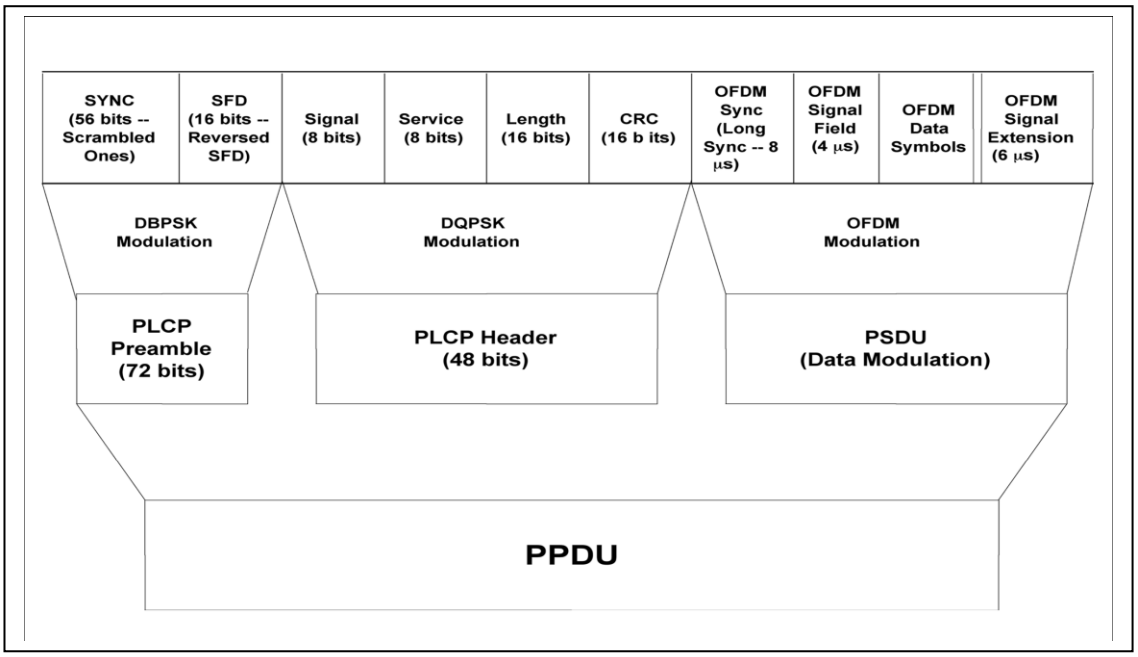
2.6.2.2 Formato de PPDU

"STA de ERP soportará tres diferente preámbulo y formatos de encabezamiento. El primero (y sobre la base con la redefinición de bits reservados definidos allí). Esto PPDU suministra la interoperabilidad con STAs para usar los 1, 2, 5.5, y 11 potencias de datos de Mbit/s; el DSSS opcional la modulación de OFDM en todas las potencias de OFDM; y el ERP opcional - la modulación de PBCC en todos ERPPBCC".[14]

El preámbulo de PLCP largo, breve y el encabezamiento de PLCP larga serán transmitidos usando 1 Mbit/s para la modulación de DBPSK. El encabezamiento de PLCP breve será transmitido usando la segunda modulación de Mbit/s.

El PSDU, el transmisor y el auricular iniciarán la modulación y serán importante(s) sugeridos por la señal de arranque con el primer octeto del PSDU. La potencia de transmisión de PSDU será puesto el DATARATE en el que el parámetro en el TXVECTOR, fue emitido con el PHY – TXSTART periodo primitivo.

GRAFICO 2.10: **FORMATO DE PPDU**
FUENTE: **Tomado del Estándar IEEE 802.11g-2003**



[14] Tomado del Estándar de la IEEE 802.11g 2003.

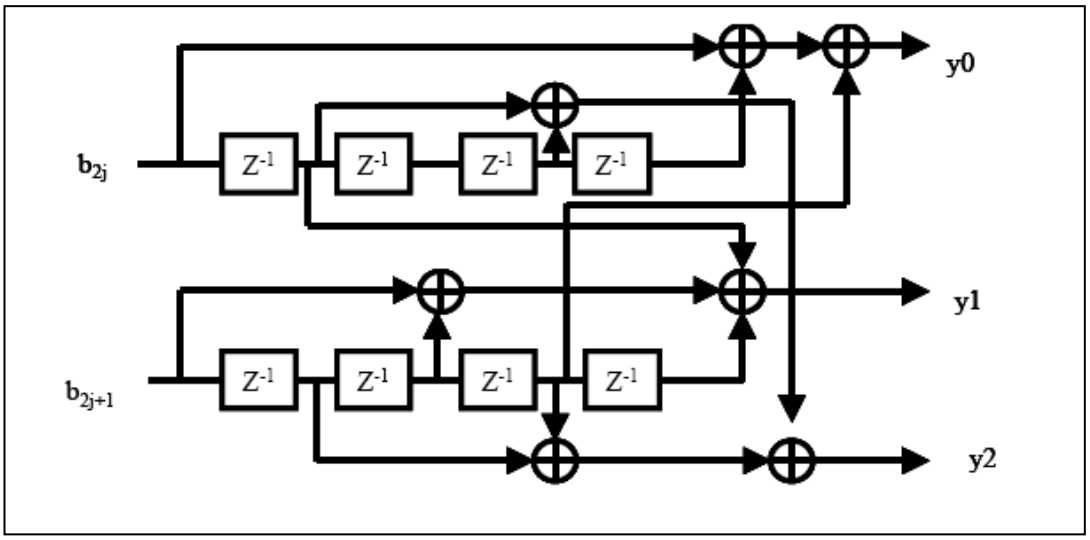
2.6.2.3 Codificador ERP - Mbit/s de 22 de PBCC y 33 formatos de Mbit/s

En el codificador de PBCC, entrante los datos son codificados primero con una clave de combinación de archivo binario de paquete. Una tapa clave (modos tan definidos en PBCC) es aplicar a los datos codificados antes de la transmisión completa.

Un codificador diagrama de bloques es mostrado en 153C de cifra. Consta de dos senderos de cuatro elementos de memoria de cada datos que bits lo introdujo, tres partes de producto son generadas. Cada 3 - la secuencia de producto de bits del codificador de combinación de archivo binario de paquete es producir un símbolo. Esto produce un caudal de proceso y transferencia de dos partes de información por el símbolo. En ERP - de PBCC.

Una ilustración del codificador del levantamiento de planos para el par de jth (= 0 de j) de partes de contribución (b2j, b2j + 1) se muestra en la figura de cifra.

GRAFICO 2.11: **CODIFICADOR DE COMBINACIÓN DE 22/33 MBIT / S ERP - PBCC**
FUENTE: **Tomado del Estándar IEEE 802.11g-2003**



La fase de la primera desportilladura complicada del 22 de la que Mbit/s PSDU será definido con respecto a la fase ultima pedazo del encabezamiento de PCLP. La fase de la primera desportilladura complicada del 33 megabytes / s PSDU serán definidos con el

respeto a la fase de la última desportilladura de la sección de interruptor de reloj. La ultima desportilladura del campo de ReSync. Los bits (y0 de y1 de y2) de los que = (0, 0,0) demostrará la misma fase como la última desportilladura. El cheque de CRC. Las demás siete combinaciones de (y0 de y1 de y2) serán definidas con respecto a esta referencia. El levantamiento de planos de productos de BCC a los 8 puntos de constelación de PSK es determinado por uno seudo - tapa aleatoria de secuencia. La secuencia en cada momento en particular es tomada como en la figura de cifra.

2.7 Metodología a ser aplicada para el aseguramiento del Sistema de Red

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

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

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de un nuevo mecanismo de seguridad llamado WPA que permitiera dotar de suficiente seguridad a las redes WLAN. También se decidieron utilizar otro tipo de tecnologías como son las VPNs para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los

datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. Pero la tecnología VPN es quizás demasiado costosa en recursos para su implementación en redes WLAN.

2.8 Seguridad WEP

2.8.1 Definición

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

WEP: Se puede habilitar o deshabilitar WEP y especificar una clave de encriptación. Wired Equivalent Privacy (WEP) proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado.

2.8.2 Características y funcionamiento

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

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

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

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

2.9 Seguridad WPA

2.9.1 Definición

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

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicó en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente madura y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible. Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

2.9.2 Características de WPA

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

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).
- **EAP**. EAP, definido en la RFC 2284 [11], es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*).
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

2.9.2.1 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48

combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

"Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad".[15]

2.9.3 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

2.9.3.1 Con servidor AAA, RADIUS normalmente.

Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

[15] Institute of Electrical and Electronics Engineers: http://www.ieee.org

2.9.3.2 Con clave inicial compartida (PSK).

Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.10 Seguridad VPN

2.10.1 Definición

Las VPN ***V**irtual **P**rivate **N**etwork* son también conocidas con el acrónimo **RPV**, (Red Privada Virtual en inglés). La **VPN** es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- **Autenticación** y **autorización**: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- **Integridad**: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza un método de comparación (Hash).Los algoritmos comunes de comparación son Message Digest (MD) y Secure Hash Algorithm (SHA).
- **Confidencialidad**: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

- **No repudio**, es decir un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

2.10.2 Despliegue de redes VPN inalámbricas en las capas altas

Una red privada virtual (VPN) es una forma de utilizar una infraestructura de telecomunicaciones pública, como Internet, para ofrecer a las oficinas o los usuarios individuales remotos un acceso seguro a la red de su organización. Ya que las redes 802.11 utilizaban bandas de frecuencia libres y usuarios imprevistos pueden acceder a ellas accidentalmente o con mala intención, las redes inalámbricas son buenos candidatos para el despliegue y mantenimiento de redes VPN. Mientras que el despliegue de redes VPN sobre un medio de cable suele reducirse a los casos específicos de teletrabajadores y oficinas alejadas de una empresa, el mundo inalámbrico es completamente distinto, y desplegar una VPN puede aplicarse a cualquier enlace inalámbrico se necesita un alto nivel de seguridad. Esto incluye a las conexiones entre máquinas de una WLAN así como en los enlaces punto a punto entre puentes inalámbricos.

Una VPN es lo más opuesto a un caro sistema de líneas propias o alquiladas que solo puede utilizar una organización. El objetivo de una VPN es ofrecer a la organización las mismas prestaciones a un coste mucho menor. Compare esta solución con la conectividad inalámbrica punto a punto, que también puede sustituir a las caras líneas alquiladas.

Una red VPN funciona utilizando una infraestructura pública compartida, mientras que se mantiene la privacidad mediante procesos de seguridad y protocolos de túnel como L2TP (lLayer Two Tunneling Protocol). De hecho, los protocolos, mediante el cifrado

de datos en el extremo emisor y el descifrado en el receptor, envían los datos a través de un túnel en el que no se pueden introducir datos que no se haya cifrado correctamente.

2.10.2.1 Motivos para el despliegue de una VPN

Las motivaciones que dan origen a la creación de una VPN son muy variadas, desde una reducción de costes a la privacidad de la comunicación. La parte común consiste en la virtualizaciòn del proceso de comunicación utilizando medios modernos para transferir datos con seguridad.

La ventaja básica de la comunicación VPN reside en una reducción de costes para la interconexión des sitios remotos. La alternativa actual a las soluciones VPN es adquirir una alquilada o añadir un servidor de acceso remoto (RAS). Las líneas dedicadas suelen instalarse para aplicaciones criticas para el objetivo de la Universidad que necesita garantizar una taza de datos muy alta entre os nodos, cuando la transferencia de datos sobre redes publicas de datos (redes PDN) no se ve fiable y no se puede garantizar la disponibilidad de ese servicio. La instalación de enlaces inalámbricos unto a punto puede ser otra alternativa barata, pero teniendo en cuenta los ataque.

2.10.3 Vista general de las Topologías VPN

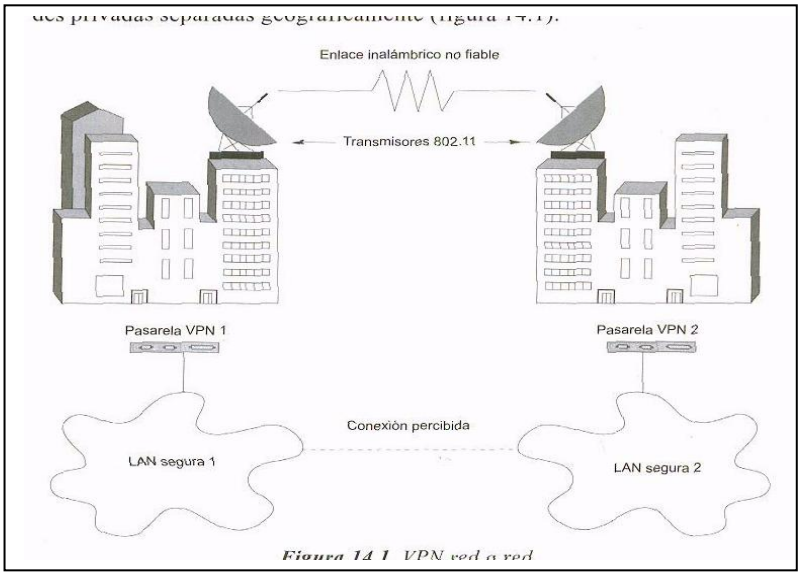
Existen varias formas de certificar redes VPN, pero los tres tipos de diseño principales son red a red, máquina a red y máquina a máquina.

2.10.3.1 Red a Red

También suele denominarse de sitio a sitio. Este término (o su forma original, network to network) se utiliza para describir un túnel VPN entre dos redes privadas separadas geográficamente. Este tipo de VPN suele utilizarse cuando hay que conectar las redes LAN a través de una red publica para que los usuarios de ambas redes puedan acceder a los recursos que se encuentren en la otra, como si estuvieren dentro de la misma red domestica. Una ventaja importante de esta configuración es que ambas redes quedan

unidas y el funcionamiento de las paralelas VPN resulta transparente para los usuarios finales.

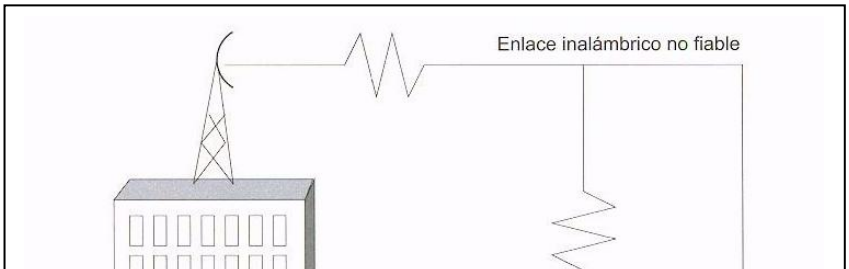
GRAFICO 2.12: VPN RED A RED.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.10.3.2 Maquina a Red

El caso de máquina a red (en su forma original, host-to network) se produce cuando existen usuarios remotos que se conectan a la red corporativa a través de Internet. El cliente móvil establece en primer lugar una conexión con Internet y después inicia una petición para establecer un túnel cifrado con la pasarela VPN corporativa. Una vez que se completa la autentificación, se establece el túnel sobre una red pública y el cliente pasa a ser otra máquina más de la red inetrena. Podría tratarse de una alternativa viable al despliegue de un servidor RADIUS, una base de Datos de usuario y una infraestructura 802.1X. La topología VPN de máquina a red asume que las máquinas inalámbricas conectadas mediante las VPN pueden acceder a distintas redes, como Internet, a través del conectador VPN, pero no pueden comunicasen con otras maquinas inalámbricas que formen parte de la misma WLAN.

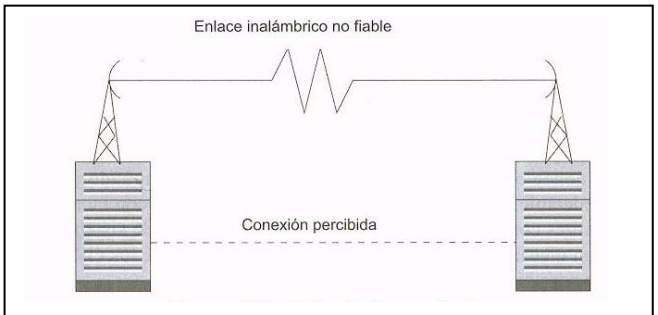
GRAFICO 2.13: MAQUINA A RED.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.10.3.3 Maquina a Maquina

La situación Maquina a máquina (en su forma original, host-to-host) es la menos habitual de las tres. Implica a dos maquinas que participan en la comunicación cifrada y sin cifrar. En esta configuración, se establece el túnel entre las dos máquinas, y todas las comunicaciones se encapsulan dentro de las VPN. La aplicación de este tipo de redes no es muy común, pero un ejemplo factible podría ser un servidor remoto de almacenamiento de copias de seguridad en una ubicación geográfica distante.

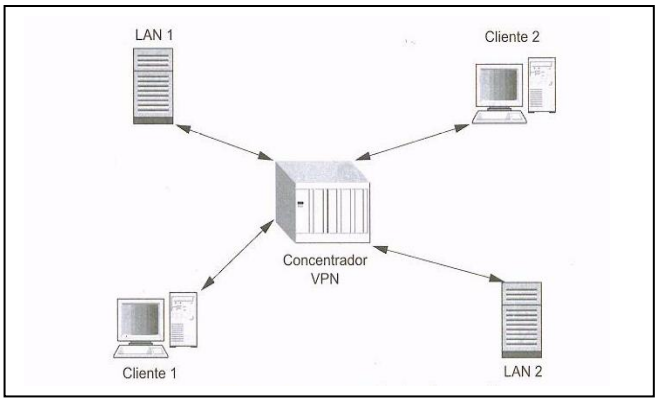
GRAFICO 2.14: MAQUINA A MAQUINA.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.10.3.4 Estrella

La topología estrella es la más habitual. Se utiliza un concentrador VPN que tiene establecido un túnel con el cliente remoto. Para que cada una de la s maquinas se comunique con las demás, los datos deben pasar de la máquina remota A al concentrador VPN y, después, del concentrador VPN a la maquina remota B. El concentrador debe ser capaz de soportar un número suficiente de conexiones simultáneas.

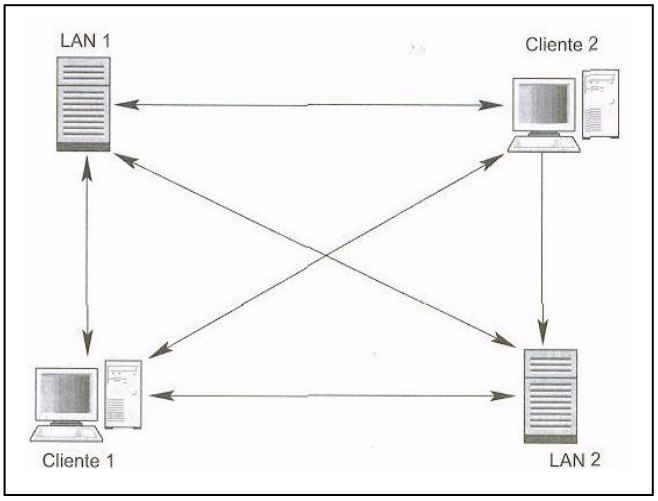
GRAFICO 2.15: VPN CON TOPOLOGIA DE ESTRELLA
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.10.3.5 Malla

En la topología de malla, cada uno de los nodos se conecta directamente mediante un túnel con otro nodo de la red, creando, una maraña de interconexiones. Este tipo topología elimina los imnconvenietes de la topología de estrella, pero presenta la desventaja de un gran aumento en el tiempo de mantenimiento y en las dificultades para añadir nuevos nodos en la red.

GRAFICO 2.16: VPN CON TOPOLOGIA DE MALLA
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.11 Logros o Insuficiencias observadas en el Sistema Actual

2.11.1 Análisis de la Situación Actual de la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi

Actualmente la Dirección de Servicios Informáticos cuenta con tecnología de punta la misma que está siendo subutilizada ya que se a implementado la red inalámbrica, pero no se encuentran trabajando para lo que fueron diseñados esto ocurre por la escasa seguridad que se brinda en la red de la Universidad y mientras no se implemente seguridades no podría mejorar el panorama, a continuación se detalla en breve resumen las respectivas pruebas realizadas de la red inalámbrica en la Universidad, al momento

de desarrollar la presente aplicación, tomaremos en cuenta que el campus se encuentra en pleno funcionamiento de forma física sus instalaciones mas no la parte tecnológica.

2.11.1.1 Funcionamiento de las redes de área local inalámbricas (WLAN, Wireless Local Área Network)

Las redes inalámbricas WLAN en la Universidad Técnica de Cotopaxi se encuentra en perfecto funcionamiento aunque no hay mayor acceso de usuarios por desconocimiento, pero se cree que están ganando mucha popularidad, ya que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Es así que al encender el Wireless en nuestro PC Portátil, nos damos cuenta que con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece una conexión automática creando nuevas aplicaciones añadiendo flexibilidad ala red, y lo más importante incrementa la productividad y eficiencia en la Universidad donde está instalada.

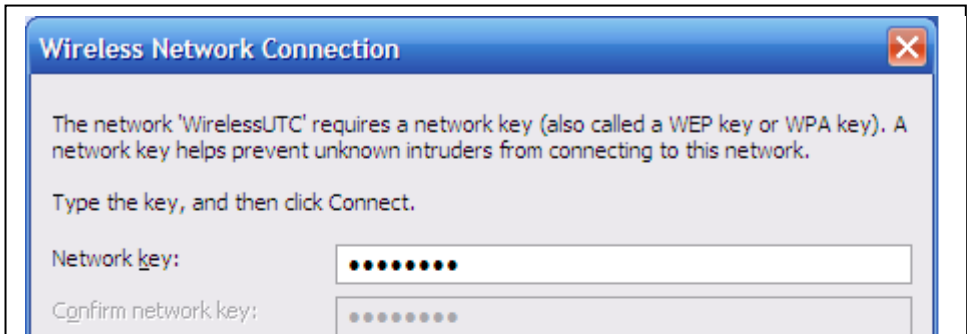
GRAFICO 2.16: RECONOCIMIENTO DEL WIRELESS UTC
FUENTE: GRUPO INVESTIGADOR.

Al continuar con la conexión nos podemos dar cuenta de que para acceder a la red se requiere de una contraseña, que es parte de la seguridad anteriormente WEP que no brinda mucha garantía hoy en día cambiada por la implementación de seguridades WPA, dichas contraseñas están asignadas en el Campus San Felipe de la Universidad Técnica de Cotopaxi de la siguiente manera:

Bloque B: 9vuc7UTC

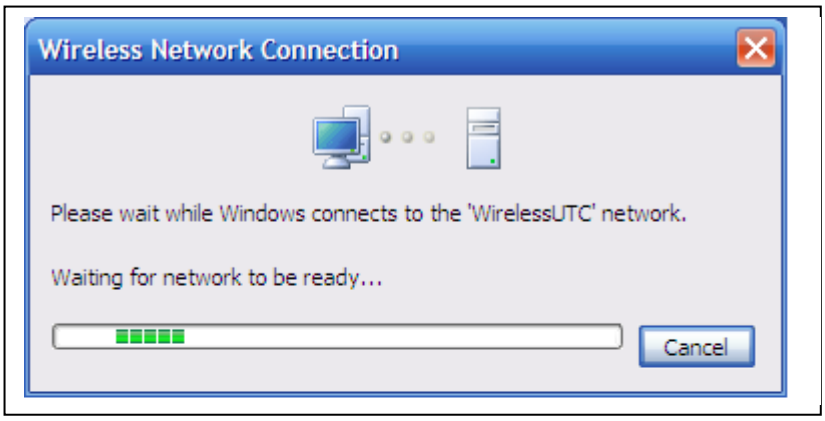
Bloque C: Bcvc7UTC

GRAFICO 2.17: CLAVES DE SEGURIDAD WPA EN LA UTC
FUENTE: GRUPO INVESTIGADOR.



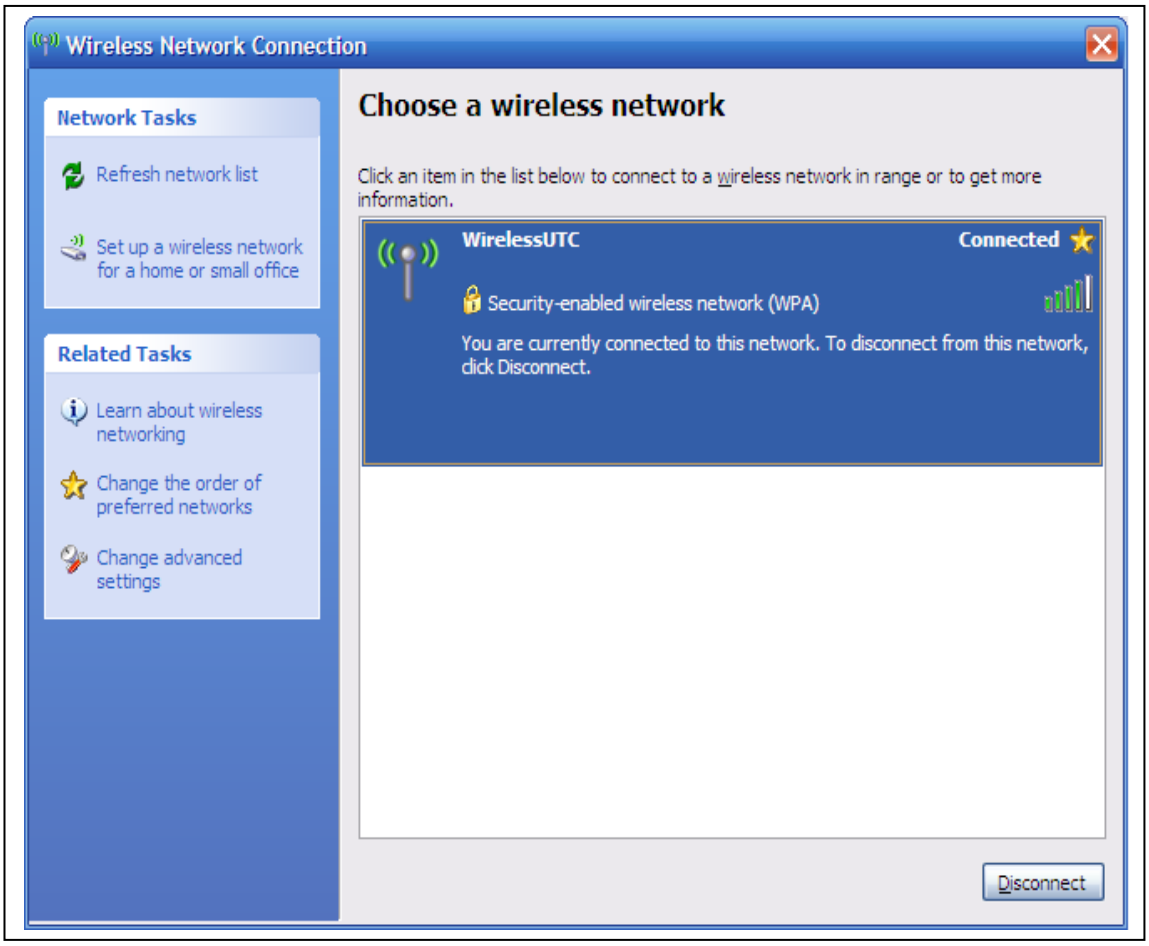
Se puede realizar una comparación al momento de acceder a la red inalámbrica tanto en el bloque B como en el Bloque C del campus San Felipe de La Universidad Técnica de Cotopaxi se lo hace en la misma forma la única diferencia es el uso distinto de contraseñas para cada bloque y el funcionamiento de la red inalámbrica es el mismo.

GRAFICO 2.18: TIEMPO DE ESPERA EN LA CONEXIÓN WIRELEES UTC
FUENTE: GRUPO INVESTIGADOR.



Una vez que logramos Conectarnos a la red inalámbrica, comprobamos que el usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de campus Universitario e inclusive puede tener acceso al Internet configurando el Servidor Proxy con el numero de IP y el puerto a velocidades de 11 Mbit/s, o superiores. Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

GRAFICO 2.19: SEÑAL DE CONEXIÓN DEL WIRELEES UTC
FUENTE: GRUPO INVESTIGADOR.



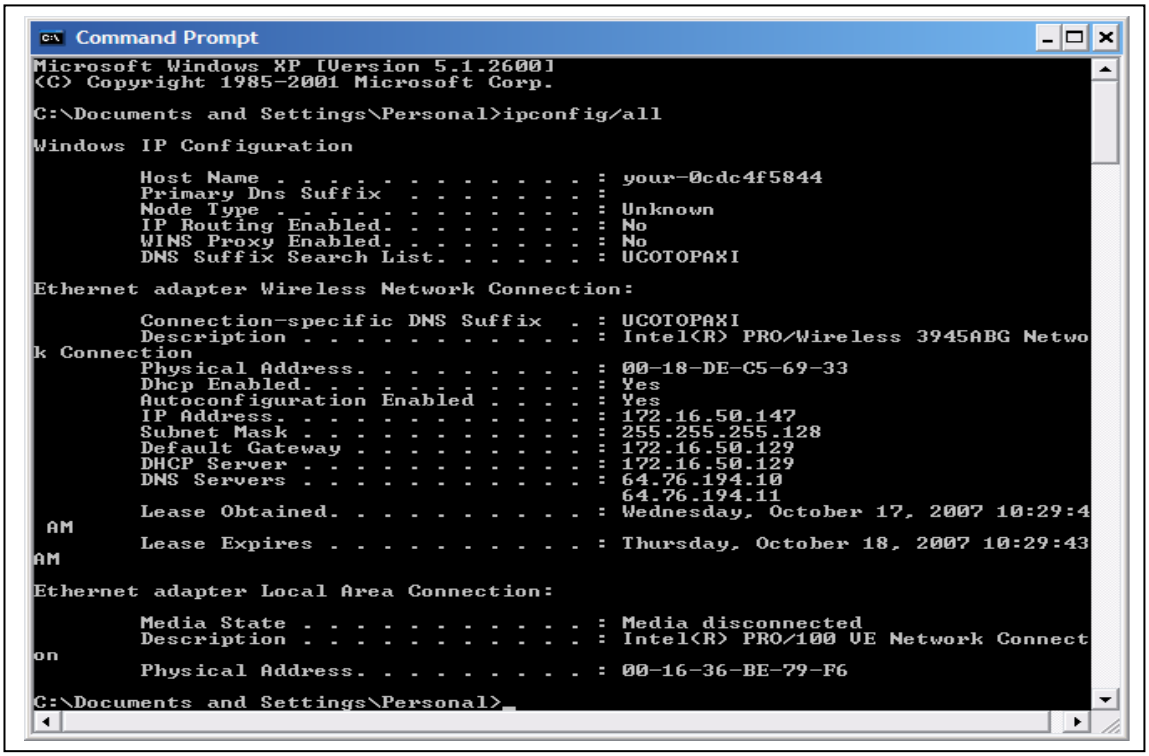
2.11.1.2 Comprobación de las redes de área local inalámbricas (WLAN, Wireless Local Área Network) mediante el proceso de Ejecución

Para realiza la ejecución se utiliza el programa ejecutar al cual accedemos con la palabra CMD en el cual se observa la ventana que permitirá realizar la respectiva comprobación, a continuación se muestra las pruebas realizadas con diferentes comandos:

2.11.1.2.1 ipconfig/all

Al ejecutar este comando ipconfig/all se puede dar cuenta que la red inalámbrica se encuentra en perfecto funcionamiento, también se destaca las respectivas características:

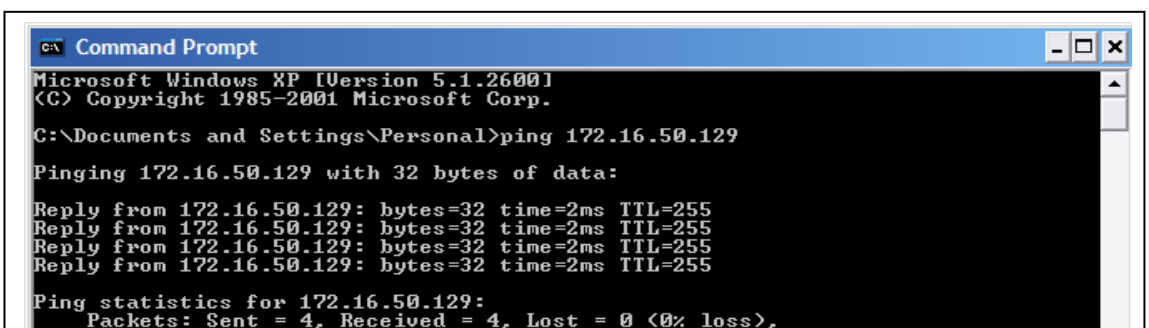
GRAFICO 2.20: EJECUCION DEL IPCONFIG/ALL UTC
FUENTE: GRUPO INVESTIGADOR.



2.11.1.2.2 ping 172.16.50.129

También se puede mandar a ejecutar haciendo ping el número de la IP en este caso la 172.16.50.129 que es el ping asignado para comprobar que ya se encuentra conectado al puerto de salida del servidor, el cual apreciamos a continuación:

GRAFICO 2.21: EJECUCION DEL PING UTC
FUENTE: GRUPO INVESTIGADOR.



2.12 Análisis de los resultados obtenidos de las Fuentes de Información Primaria, Criterios de los Docentes y Estudiantes

2.12.1 Métodos Y Técnicas

Para la obtención de la información de la red de la Institución, en primer lugar se tomo en consideración el Área de Servicios Informáticos.

2.12.1.1 Procesos Del Área De Servicios Informáticos

La información fue descrita en base a una conversación con los responsables directos como son el Director de Servicios Informáticos y el Operador de los Centros de Cómputo.

La asistencia personal fue el principal método de investigación que en ocasiones debía ser permanente y en otros esporádicos en las instalaciones de la Dirección de Servicios Informáticos, con el propósito de consolidar información fiable y suficiente, a la vez esclarecer ciertas dudas.

La información conseguida de las entrevistas planificadas y repentinas se utilizó con el fin de comparar el desarrollo del Departamento de Servicios Informáticos. Para lo cual fue necesario conocer cada una de las actividades realizadas por las personas responsables de la misma, se necesito observar como se desarrolla las actividades de esta área con la visita al departamento de Servicios Informáticos, en el cual laboran dos personas, se obtuvo documentación de las actividades que cada uno de ellos realiza.

El Director es el encargado de manejar los recursos de la red.
El Operador de Centros de Computo es el encargado del manejo de la Página Web de la Institución.

De la conversación mantenida se pudo llegar a la conclusión de que el departamento de servicios informáticos no ha implementado ningún tipo de seguridad en la red inalámbrica.

Razón por la cual el grupo investigador tomando en cuenta estos criterios por parte de los administradores de la red, procedió a realizar la aplicación de este proyecto de tesis, para que de esta manera se de el mejoramiento y la funcionalidad del servicio que presta la red de la Universidad Técnica de Cotopaxi.

2.13 Beneficios que tendrá la Red Inalámbrica de la Universidad Técnica de Cotopaxi con la implementación de seguridades bajo los estándares 802.11 b y g.

Se puede decir que gracias a la implementación de seguridades se han logrado optimizar recursos técnicos, humanos y financieros de esta manera proporcionan a los usuarios tener acceso a la información en tiempo real y en forma segura en cualquier lugar dentro de la organización.

Los beneficios de Wi-Fi en términos de movilidad y flexibilidad, unido al aumento de velocidad y a la reducción en el coste de las tarjetas de red, lo hacen el más recomendado y utilizado.

Al contar con la implementación de seguridades en las red inalámbrica a llevado a que ya no exista pérdida y alteración de la información, que exista libertad de movimientos, espacio suficiente causando grandes mejoras, como la reubicación de las estaciones de trabajo y por ende evita el bloqueo de servidores, cambio de direcciones IP de las maquinas ocasionando un correcto análisis, monitoreo y control de trafico de la información a los administradores de la red inalámbrica en la Institución.

Al desarrollar este tema se propone dar solución a los problemas como detectar mal servicio, congestionamiento, invasión, daños en la red, interferencias, deficiencia en el servicio de Internet y acceso a los recursos compartidos en forma ilegal, debido a que ésta por ser de carácter tecnológico debe estar en constante actualización.

2.14 Ventajas y desventajas encontradas al poner en marcha la seguridad en la red inalámbrica bajo los estándares 802.11 b y g.

- Al mantener una compatibilidad los estándares 802.11b y g con versiones anteriores protege la inversión de los Administradores y usuarios de la red Inalámbrica de la Universidad Técnica de Cotopaxi.
- Con la utilización del estándar 802.11g se puede conseguir velocidades de datos más elevados y con mayor alcance que otros productos analizados con tecnología diferente.

- Permitirá al administrador y al usuario instalar fidelidad inalámbrica en los meses y años siguientes. Esta implementación de seguridades será de un alto benéfico para los estudiantes universitarios y a los administradores de la red inalámbrica de la Institución.
- Con la aprobación de la nueva versión 802.11g se ha conseguido que el actual índice de transmisión de datos de 11 Mbit/s empleado por la versión "802.11b", pase a ser de 54 Mbit/s, lo que permitirá dar servicio a 4 ó 5 veces más de usuarios y extender el uso de las **redes wireless 802.11**, conocido popularmente como WIFI**,** a servicios bastante demandados como la transmisión inalámbrica de video-multimedia y la difusión de MPEG.
- La principal ventaja en términos de seguridad es que en una misma zona de cobertura pueden trabajar simultáneamente tres puntos de acceso, cada uno de ellos con un alcance para interiores de unos 90 m a 1 Mbit/s y de unos 30 m a la tasa máxima de 11 Mbit/s, esto permite garantizar el flujo de la información que circula en la red inalámbrica de la Universidad.

CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DEL DISEÑO E IMPLEMENTACION DE SEGURIDADES EN LA RED INALAMBRICA.

3.1. Diseño y Factibilidades de las Redes Inalámbricas

En la actualidad en la Universidad Técnica de Cotopaxi nos encontramos interconectados el bloque académico B y el bloque C donde se encuentra el comedor universitario y la biblioteca de forma inalámbrica a un muy buen ancho de banda el mismo que oscila en los parámetros internacionales como son de 56 KBPS hasta 108 KBPS de acuerdo al trafico y al numero de usuarios que tenga la red de la universidad, es indispensable hacer notar que al tener una interconexión inalámbrica debemos tener seguridades para cuidar la carga de la red ya que al tener solamente 512 KBPS de ancho de banda en la conexión a Internet de forma simétrica resulta que no abastece para el numero de estudiantes que tiene la institución y el numero de investigadores que utilizan este recurso en horas pico.

Una adecuada distribución de los equipos de enlace se hace urgente ya que al tener estas antenas de gran capacidad y de una amplia cobertura hace que pueda ser utilizada por personas ajenas a nuestra institución.

Es claro notar que las antenas se encuentran ubicadas en sitios estratégicos de los dos edificios el mismo que tiene vista para los cuatro puntos cardinales, y pueden ser replicas con otros dispositivos de cobertura inalámbrica con switch y Access Point, en caso de que sea necesario replicar en sitios inaccesible de cada uno de los edificios, hemos podido notar que esta cobertura no abastece al edificio antiguo ya que tiene algunas interferencias, por lo que se haría necesario la implementación de dispositivos que repliquen estas señales o que a su vez la adquisición de una o mas antenas que tomen la señal de los servidores y repliquen a sitios de la Universidad que se encuentren anegadas al servicio de red inalámbrica.

3.1.1. Factibilidad Técnica.

La implementación de seguridades en las redes inalámbricas de la Universidad Técnica de Cotopaxi está basado en un amplio porcentaje en lo que manifiestan los estándares de la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), los mismos que se utilizo el

802.11 b y el 802.11g que son los mas utilizados en nuestro medio, por ser para redes de área local que dicen básicamente lo siguiente:

3.1.1.1 Implementación de seguridades mediante el estándar de la IEEE 802.11b

Tomando en consideración que el estándar 802.11b es un medio seguro notificado por la IEEE, nosotros hemos utilizado el mismo para garantizar la seguridad del flujo de la información en la red Inalámbrica del Bloque B, C; Campus San Felipe de la Universidad Técnica de Cotopaxi, además por sus diferentes bondades en cuanto tiene que ver con las características que presenta el mismo como son: su alta velocidad para redes WLAN, ofrece una tasa de transmisión de hasta 11 Mbit/s, que puede llegar a compartirse entre doce conexiones de un mismo punto de acceso.

Además, en una misma zona de cobertura pueden trabajar simultáneamente tres puntos de acceso, cada uno de ellos con un alcance para interiores de unos 90 m a 1 Mbit/s y de unos 30 m a la tasa máxima de 11 Mbit/s. La tasa de transmisión puede seleccionarse entre 1, 2, 5,5 y 11 Mbit/s, característica denominada DRS (Dynamic Rate Shifting), lo cual permite a los adaptadores de red inalámbrica de la Institución reducir las velocidades para compensar los posibles problemas de recepción que puedan generarse por las distancias o los materiales que deba atravesar la señal (paredes, techos, ventanas, etc.), especialmente en el caso de interiores ya que el Bloque B por ejemplo es de cuatro plantas y el Bloque C de 2. En el caso de espacios abiertos, los alcances pueden aumentar hasta 120 m (a 11 Mbit/s) y 460 m (a 1 Mbit/s). Los sistemas basados en el estándar IEEE 802.11b se caracterizan por un conjunto de canales de 22 MHz solapados entre sí, siendo fija la asignación de canales a cada punto de acceso. La planificación por defecto debe realizarse con estos canales, ya que aunque es posible utilizar canales solapados, esto requiere un análisis previo bastante detallado para determinar el efecto de la perturbación producida por el canal adyacente.

El estándar 802.11b se ha desplegado claramente por todo el Bloque B y C.

Ocasionando beneficios en términos de movilidad y flexibilidad, unido al aumento de velocidad y a la reducción en el coste de las tarjetas de red, lo ha convertido también en una opción muy atractiva para cuando se implemente la red inalámbrica en los futuros bloques de la Universidad Técnica de Cotopaxi.

3.1.1.2 Implementación de seguridades mediante el estándar de la IEEE 802.11g.

En cuanto tiene que ver al estándar 802.11g ratificado por la IEEE se hace imprescindible utilizarlo conjuntamente con el estándar 802.11b para reforzar la seguridad que requiere la red inalámbrica de los Bloques B y C de la Universidad Técnica de Cotopaxi, El hecho de utilizar la banda de 5 GHz provoca que los productos 802.11g sean completamente compatibles con los productos 802.11b.

Por ello se ha utilizado el estándar 802.11g para analizar la posibilidad de desarrollar una extensión del estándar 802.11b en los posteriores bloques que se están construyendo en la Institución, que permitirá velocidades superiores a los 20 Mbit/s en la banda de 2,4 GHz. El estándar 802.11g utiliza tecnología OFDM, implementando al mismo tiempo las modalidades 802.11b, manteniendo de este modo la compatibilidad con el equipamiento 802.11b. Luego en términos de velocidad y alcance, las prestaciones del estándar 802.11g son mejores que las de cualquiera de las alternativas que se presentan.

También podemos mencionar que el estándar 802.11g esta operando en los actuales momentos en los Bloques B y C del Campus San Felipe en completa compatibilidad con el estándar 802.11b sin necesidad de licencia alguna, lo cual no quiere decir que deje de ser una norma de seguridad confiable al momento de garantizar el verdadero flujo de la información entre departamentos.

Las seguridades que se pudo analizar fueron tanto el WPA como WEP, servidores RADIUS, la utilización de VPN (Virtual Prívate Network), pero por facilidad de

implementación y la cantidad de información que se dispone tanto en libros como en Internet y por el tipo de encriptado que posee, tanto los administradores de la red como el grupo investigador se inclino por el WPA.

3.1.1.3 Mejoras propietarias al protocolo WEP y el uso de WEP.

Las vulnerabilidades más anunciadas de 802.11 son las inseguridades del protocolo WEP. Una vez realizado un análisis en la seguridad de la red Inalámbrica de la Universidad Técnica de Cotopaxi, hemos detectado las debilidades criptográficas que presenta WEP en relación con la reutilización del espacio de vectores de inicialización de claves y el inseguro algoritmo de generación de claves a partir de cadenas. También existen algunos problemas de gestión de claves muy bien conocidos:

- Todas las implementaciones de cifrado simétrico tienen problemas con la distribución segura de las claves. El protocolo WEP no es una excepción, en el diseño original se suponía que WEP iba a defender pequeñas redes en una sola celda. Ya que las redes inalámbricas que tenemos actualmente en la Universidad suelen involucrar a cientos de máquinas móviles, lo que hace que la distribución y el cambio manual de las claves WEP sean una pesadilla.

- La clave WEP proporciona una autentificación de dispositivos y no de usuarios. Ya que cuando el cracker roba o encuentra un dispositivo perdido, conseguirá acceso a la red inalámbrica de la Institución con el que este dispositivo este configurado para conectarse.

- Todas las máquinas de la red tienen la misma clave WEP. Razón por la que Husmear la red WLAN es tan sencilla como escuchar paquetes en una red Ethernet compartida, y puede lanzarse inclusive otros ataques demoledores, tal y como se mostró en las pruebas realizadas en cada uno de los bloques B y C, Ver Anexos.

Conscientes de este problema, aprovechando la publicación de la IEEE como un mecanismo opcional de seguridad, denominado WPA, en la norma de redes inalámbricas 802.11, nosotros hemos buscado como una gran alternativa para solucionar los problemas de seguridad en el verdadero flujo de la información a esta tecnología.

3.1.1.4 WPA la solución al WEP.

En gran parte de este capitulo se trata tanto a WPA como a la WEP dinámica, existen dos puntos principales en esta documentación en los que se ofrecen distintas instrucciones:

3.1.1.4.1 Creación de una directiva de acceso remoto de IAS para WLAN con WPA.

Para utilizar la protección de WLAN con WPA en lugar de WEP dinámica, debe establecer el valor de tiempo de espera de la sesión en ocho horas (y no en 60 minutos). WPA dispone de un mecanismo integrado que genera claves de cifrado de las redes inalámbricas WLAN, de forma que no necesita forzar a los usuarios a volver a autenticarse con frecuencia. Un valor de ocho horas es suficiente para asegurar que los usuarios dispongan de credenciales actualizadas válidas (por ejemplo, garantiza que un usuario que no permanezca conectado durante un tiempo excesivo una vez que la cuenta se ha deshabilitado). En entornos de alta seguridad, puede reducir este valor de tiempo de espera, si es necesario.

3.1.1.4.2 Para modificar la configuración del perfil de la directiva de acceso inalámbrico.

1. En el complemento MMC del Servicio de autenticación de Internet, abra las propiedades de la directiva Permitir acceso a LAN inalámbrica y haga clic en Modificar perfil.

2. En la ficha Restricciones de marcado del campo Minutos que el cliente puede estar conectado (tiempo de espera de sesión), escriba *480* (480 minutos u 8 horas).
3. En la ficha Avanzadas, agregue el atributo Ignorar propiedades de acceso telefónico del usuario y establézcalo en True; a continuación, agregue el atributo Acción-Terminación y establézcalo en RADIUS Request.

También debe modificar el tiempo de espera de la sesión en el punto de acceso inalámbrico para que se halle en el mismo nivel del valor de tiempo de espera establecido en este procedimiento (o lo supere).

3.1.1.5. Protocolo WPA (Wi-Fi Protected Access)

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios en todo el mundo para el caso en nuestra Universidad Técnica de Cotopaxi se hace imprescindible ya que WEP no puede proporcionar mayor seguridad.

Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un usuario se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, para permitir el tráfico de validación entre el usuario y una máquina de la de local. Una vez que se ha validado a un usuario es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los usuarios WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS que describimos más adelante.

WPA utiliza TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

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

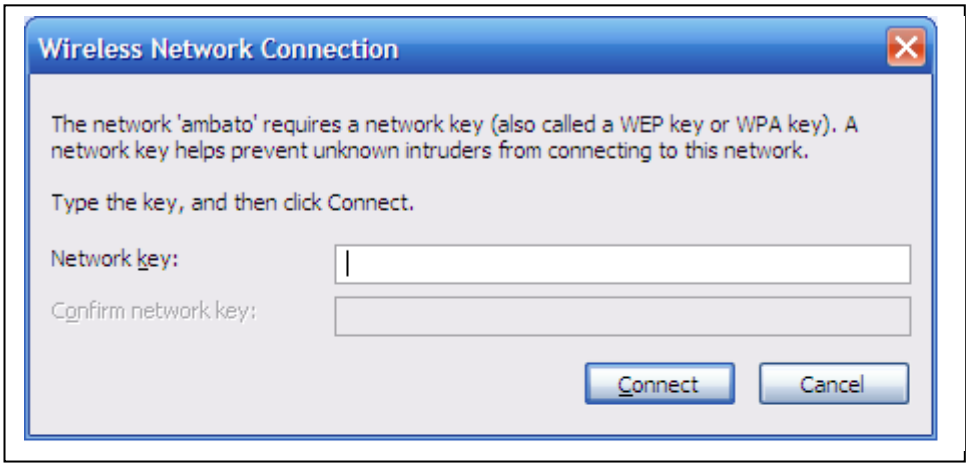
3.1.1.5. Comparación del WEP frente al WPA

El grupo investigador cumpliendo con los objetivos propuestos ha realizado muchas prácticas y pruebas que nos permitió demostrar científica y tecnológicamente las diferencias existentes entre la tecnología WEP (anteriormente implantada en la Universidad Técnica De Cotopaxi) y la tecnología WPA hoy en día implementada para garantizar el real funcionamiento de la red inalámbrica, para lo cual no solamente se tomo referencia a la Universidad en sus respectivos Bloques B y C sino que también se realizo comparaciones para un mejor entendimiento con otra institución como es el Mall de los Andes que se encuentra ubicado en la Ciudad de Ambato.

Para tener mayor certeza en la obtención de resultados primeramente procedimos a realizar las primeras practicas, las mismas que lo hicimos en el Centro comercial Mall de los Andes ubicado en la Ciudad de Ambato en el cual nos pudimos dar cuenta que utilizan tecnología WEP el cual no brinda ningún tipo de seguridad, ya que cualesquier usuario que ingresa al Comercial a la obtención de sus servicios y tan solo con llevar su computador portátil al mencionado local y encender su Wireless accede a la red

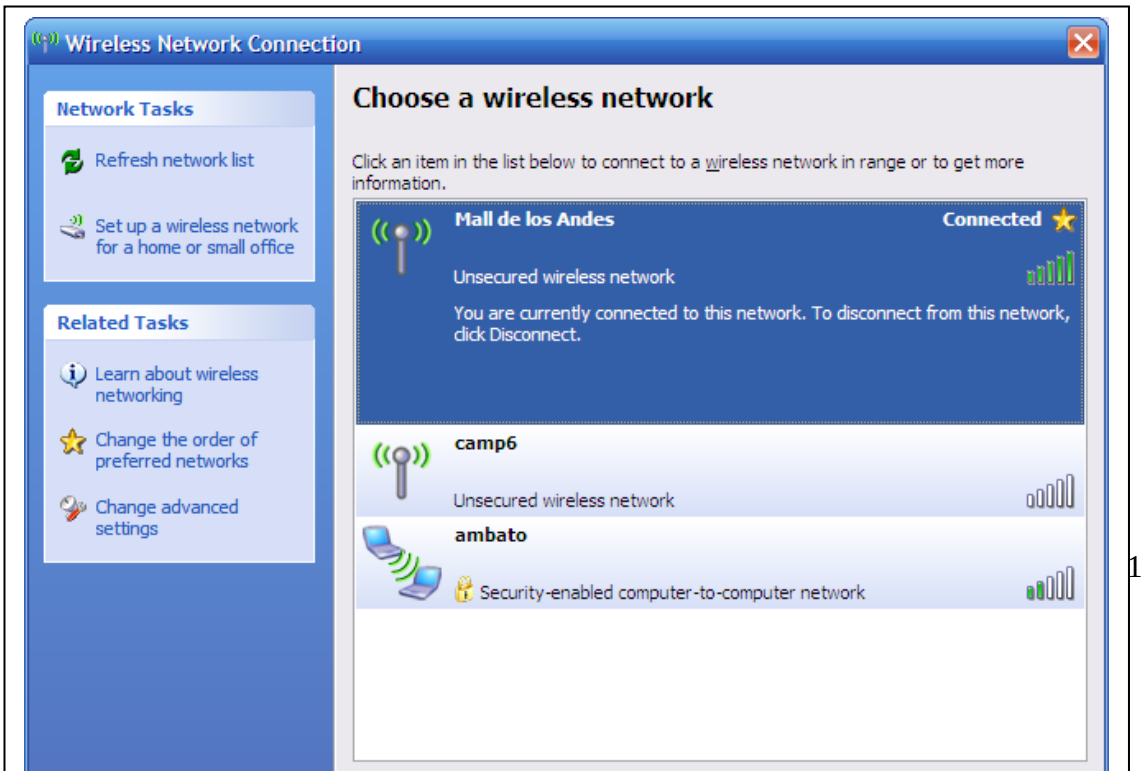
inalámbrica y a los servicios de Internet sin ningún tipo de restricción ya sea a través de claves o contraseñas como podemos observar a continuación.

GRAFICO 3.1: CONEXIÓN WIRELESS SIN CLAVE WPA- MALL DE LOSANDES.
FUENTE: BIBLIOTECA PERSONAL



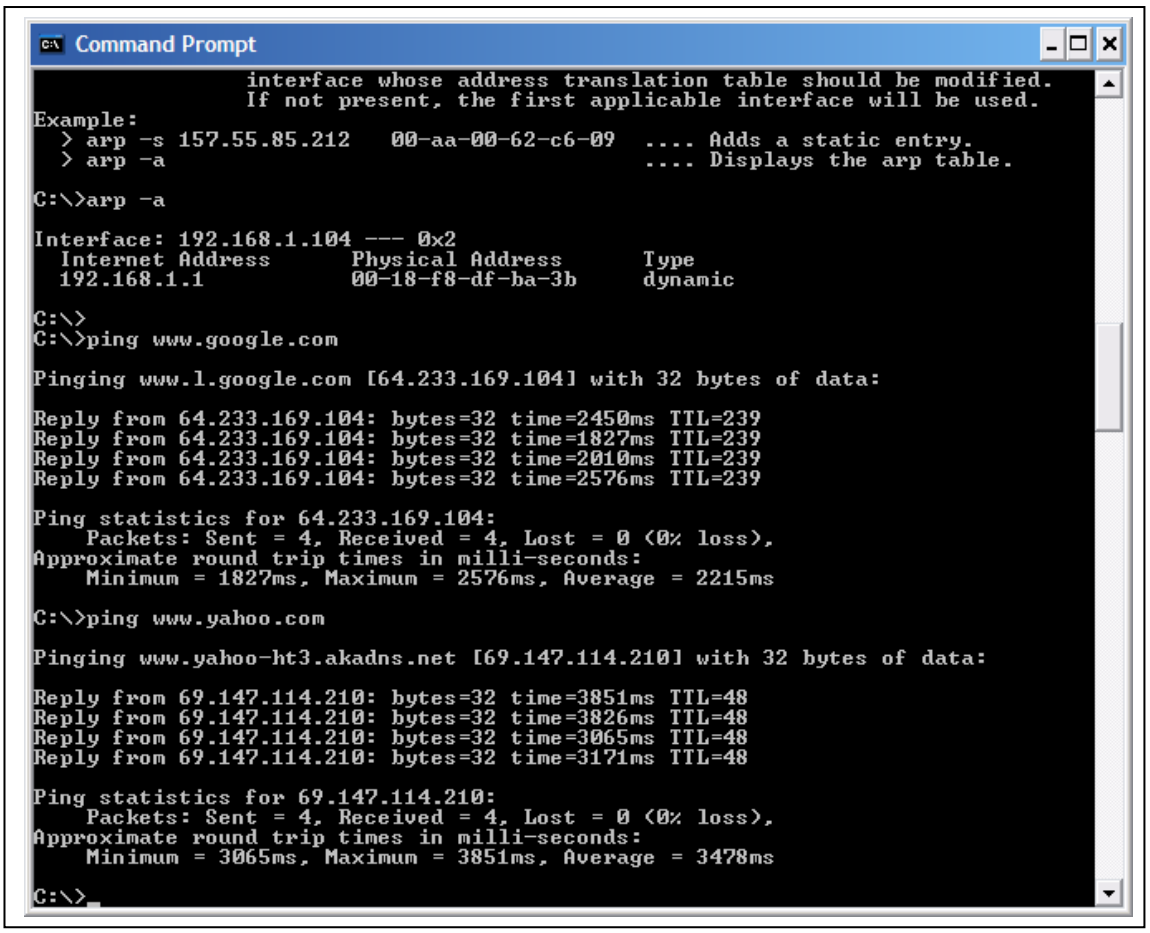
Sin ingresar ninguna clave los clientes se conectan a la red y acceden al servicio de Internet y nos podemos dar cuenta que la red esta distribuida por campos para el caso el nuestro se realizo en el campo 6, con un despliegue de señal rápida y nítida.

GRAFICO 3.2: SEÑAL DE CONEXIÓN WIRELESS MALL DE LOS ANDES.
FUENTE: BIBLIOTECA PERSONAL



También se puede comprobar que se genera una IP de manera automática, esto lo podemos observar al mandar a ejecutar el comando ipconfig/all dentro de CMD y muchas características mas que demuestran que se conecto ala red inalámbrica del Mall de los Andes, obteniendo como resultado que es muy indispensable implementar seguridades WPA en la Universidad para garantizar el verdadero flujo de la información.

GRAFICO 3.3: EJECUCIÓN DEL COMANDO IPCONFIG/ALL MALL DE LOS ANDES
FUENTE: BIBLIOTECA PERSONAL



Luego de contar con la suficiente experiencia de las pruebas realizadas en el Mall de los Andes, procedimos a practicarlas en los Bloques B y C del Campus San Felipe de la Universidad Técnica de Cotopaxi y nos dimos cuenta que utiliza tecnología de seguridades WEP que en cierta manera le da seguridad a la red inalámbrica de la institución pero no lo suficiente como para garantizar la información, por lo cual se procedió a implementar la seguridad WAP de la siguiente manera:

3.1.1.5.1 Configuración manual de WLAN en Windows XP para WPA

Mientras no se disponga de compatibilidad con el objeto de directiva de grupo en Windows Server 2003 Service Pack 1, deberá configurar WPA en el equipo cliente de forma manual. WPA es compatible con Windows XP Service Pack 1 con la descarga del usuario WPA instalada (o en Windows XP Service Pack 2). Cuando disponga de compatibilidad con el objeto de directiva de grupo, podrá utilizar el siguiente procedimiento para crear una directiva de red inalámbrica con la misma configuración.

1. Abra las propiedades de la interfaz **Red inalámbrica**. Si en la lista **Redes disponibles** aparece WLAN, selecciónela y haga clic en **Configurar** o en **Agregar** (en la sección **Redes preferidas**).
2. Escriba el nombre de la WLAN en el campo **Nombre de red (SSID)** (si no aparece ya) y, en el campo **Descripción**, escriba una descripción para la red. Si ya posee una WLAN configurada y desea ejecutarla en paralelo con la WLAN basada en 802.11de esta solución, debe utilizar un Identificador del conjunto de servicios (SSID) para la nueva WLAN. Este nuevo SSID deberá utilizarse aquí.

3. En la sección **Clave de red inalámbrica**, seleccione **WPA** (no seleccione **WPA PSK**) como el tipo de **Autenticación de red** y **TKIP** como el tipo de **Cifrado de datos**. Si el hardware es compatible, seleccione el estándar de cifrado avanzado más seguro (**AES** en lugar de **TKIP**).
4. Haga clic en la ficha **IEEE 802.11** y seleccione **EAP protegido (PEAP)** de la lista desplegable **Tipo de EAP**.
5. Haga clic en el botón **Configuración** para modificar la configuración PEAP. En la lista **Entidad emisora raíz de confianza**, seleccione el certificado de entidad emisora raíz para la entidad emisora, que es la que instaló para emitir certificados del servidor IAS (consulte el capítulo 4 para obtener más información). **S**i necesita instalar de nuevo la entidad emisora desde cero (no sólo restaurarla desde la copia de seguridad), deberá modificar la configuración del cliente y seleccionar el certificado de entidad emisora para la nueva entidad emisora.
6. Asegúrese de que selecciona **Contraseña protegida (EAP-MS-CHAP v2)** en **Seleccione el método de autenticación** y compruebe la opción **Habilitar reconexión rápida**.
7. Cierre cada una de las ventanas de propiedades haciendo clic en **Aceptar**.

3.1.1.5.2 Migración de WEP a WPA

Si ha implementado una solución WLAN segura basada en WEP dinámica y para migrar a WPA, deberá seguir los pasos que se indican en esta sección. Antes de realizar la migración, debe asegurarse de que ha implementado los elementos de compatibilidad con WPA, tanto el software (por ejemplo, el componente WPA de Windows XP) como el hardware (actualizaciones del firmware del punto de acceso y del controlador del adaptador de red). Toda referencia en este procedimiento sobre la configuración de WPA en objetos de directiva de grupo es válida solamente si estos objetos se modifican desde Windows Server 2003 Service Pack 1 o posterior.

Para realizar una migración de WEP a WPA cuando el punto de acceso admite simultáneamente WEP dinámica y WPA:

1. Configure todos los puntos de acceso inalámbrico para que admitan WEP dinámica y WPA a la vez.
2. Cree un nuevo objeto de directiva de grupo de la configuración del cliente WLAN. Cree una directiva de red inalámbrica que establezca la configuración adecuada para WPA (consulte el procedimiento de la sección "Configuración manual de WLAN en Windows XP para WPA" de este apéndice). A continuación, deshabilite el objeto de directiva de grupo de la WEP actual y habilite el de WPA para que todas las configuraciones de WPA se envíen a todos los clientes. Los clientes comenzarán a utilizar WPA en la WLAN una vez se haya actualizado el objeto de directiva de grupo. Si configura los usuarios de forma manual, deberá deshabilitar el objeto de directiva de grupo que contenga la configuración WEP, ya que, de no hacerlo, el objeto de directiva de grupo sobrescribirá la configuración WPA manual.
3. Finalmente, debe actualizar el tiempo de espera de la sesión de la directiva de acceso remoto IAS y de la sesión de usuario en el punto de acceso (tal y como se describe en la sección sobre la directiva de acceso remoto IAS anterior de este apéndice).

Para realizar una migración de WEP a WPA cuando el punto de acceso no admite WEP y WPA simultáneamente:

1. Cree un nuevo SSID de WLAN para la red WPA.
2. Modifique el objeto de directiva de grupo de la configuración de red del usuario y agregue el nuevo SSID con los parámetros de WPA (tal y como se describe en la sección "Configuración manual de WLAN en Windows XP para WPA" anterior de este apéndice). Si configura los clientes de forma manual, deberá hacerlo con el nuevo SSID y, asimismo, con la configuración de WPA para ese SSID. En cualquier caso, no quite la configuración del SSID de la WEP anterior.

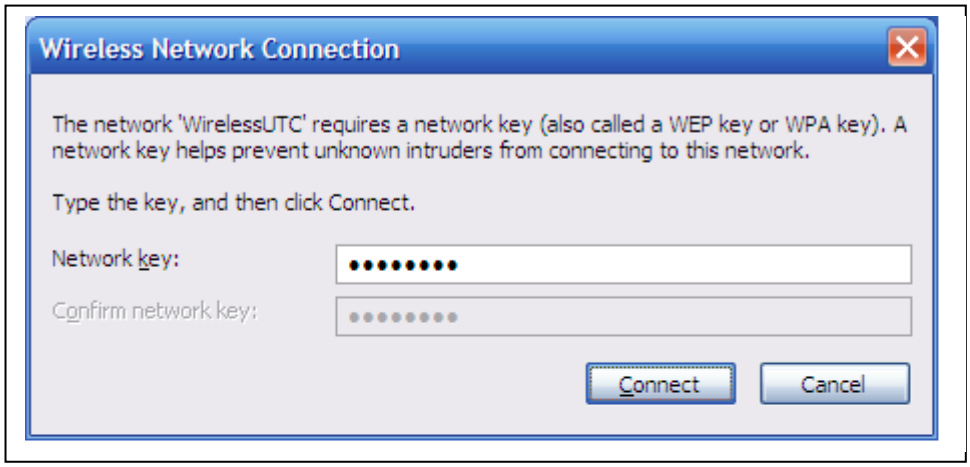
3. De forma simultánea, vuelva a configurar los puntos de acceso que admitían WEP para que sean compatibles con WPA y modifique el SSID del punto de acceso. A medida que vaya configurando cada punto de acceso, los usuarios cambiarán al nuevo SSID y utilizarán WPA.
4. Una vez que haya reconfigurado todos los puntos de acceso, podrá actualizar las directivas de acceso remoto en todos los servidores IAS. Será necesario aumentar el valor de tiempo de espera de la sesión en la directiva de acceso remoto (de 60 minutos a 8 horas) y, además, modificar la misma configuración en los puntos de acceso inalámbrico (tal y como se describe en la sección sobre la directiva de acceso remoto IAS anterior de este apéndice).
5. Una vez que ha finalizado la migración, puede quitar el SSID de la WEP del objeto de directiva de grupo.

Una vez realizado la configuración y la migración de WEW a WAP se puede verificar que la implementación de seguridades WPA nos permitirá garantizar el verdadero flujo de la información, es así que a partir de la mencionada implementación todos los usuarios que deseen acceder a la red inalámbrica de los bloques B y C del Campus San Felipe de la Universidad Técnica de Cotopaxi deberán contar con la respectiva contraseña para cada bloque tanto como el B como para el C, las cuales son diferentes contraseñas de seguridad WPA como veremos continuación:

Bloque B: 9vuc7UTC

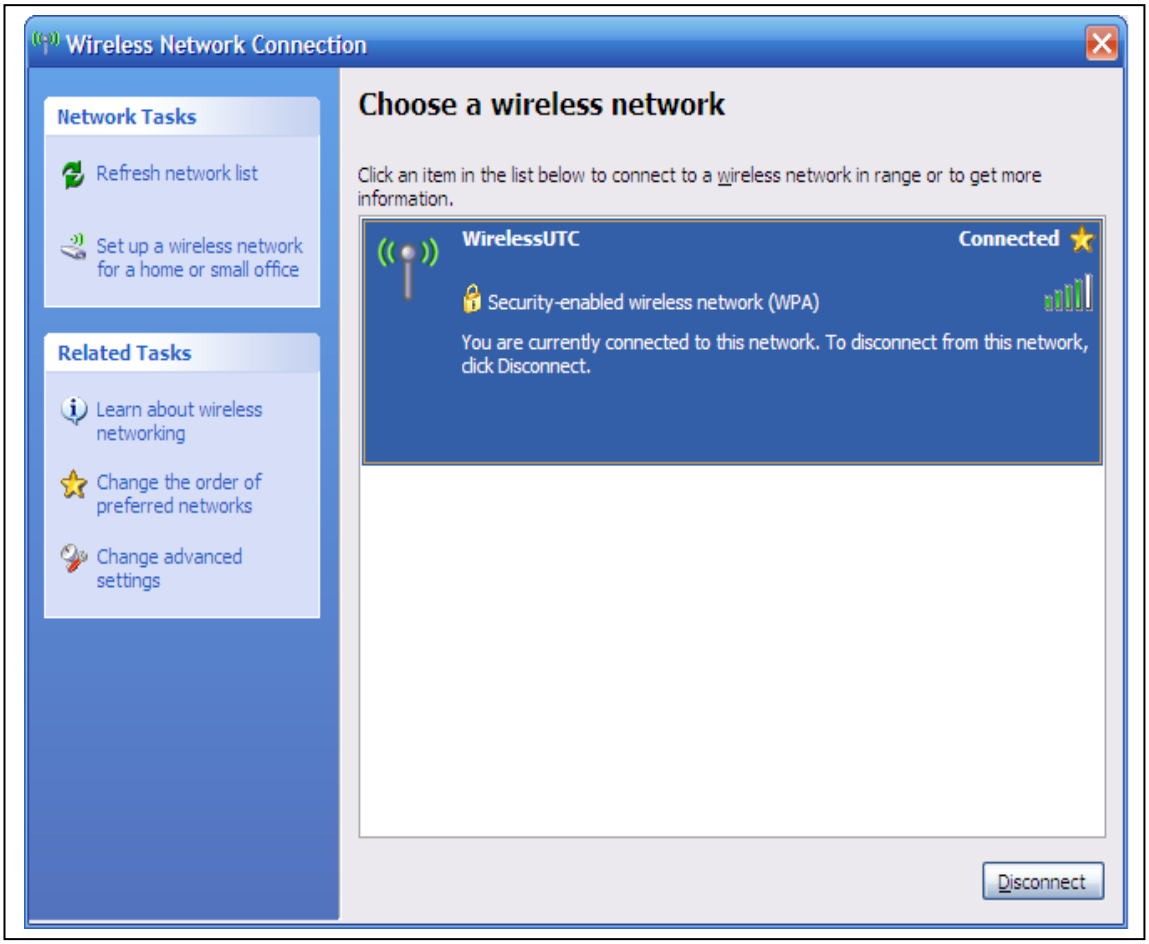
Bloque C: Bcvc7UTC

GRAFICO 3.4: CLAVE DE SEGURIDAD WPA EN LOS BLOQUES B Y C
FUENTE: GRUPO INVESTIGADOR.



Las contraseñas para acceder a cada uno de los bloques creadas por la configuración WPA son diferentes y tienen un cierto grado de dificultad ya que tienen ciertos trucos como es: la mezcla de caracteres entre números y letras mayúsculas, minúsculas el cual evitara el ingreso de intrusos a información confidencial, así como al robo del Internet tanto en el bloque B como en el C, este ultimo mas accesible ya que la red inalámbrica se extiende hasta las canchas deportivas y bien podrían personas ajenas a la universidad causar desmanes y por ende grandiosas perdidas a la institución.

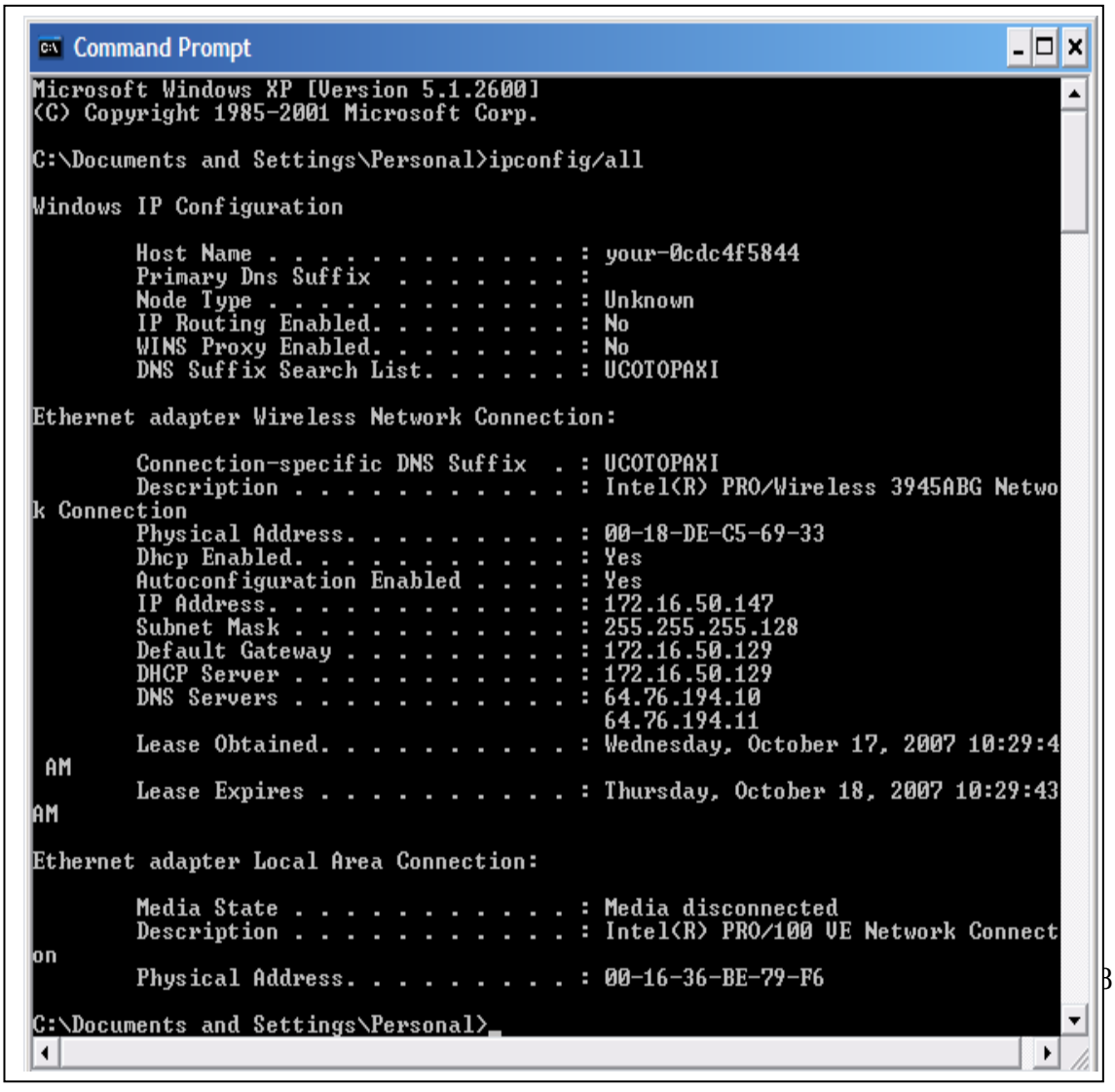
GRAFICO 3.5: SEÑAL DE LA CONEXIÓN A LA RED INALAMBRICA CON SEGURIDAD WPA UTC.
FUENTE: GRUPO INVESTIGADOR.



En comparación a otras instituciones y la misma universidad que antes utilizaban tecnología WEP hoy remplazada por WPA es una gran alternativa de cambio para el mejor desenvolvimiento de la red inalámbrica, de esta manera la Universidad Técnica de Cotopaxi se constituye en una de las pioneras en tecnología y seguridad siendo de gran utilidad para el desarrollo y progreso de la sociedad. A continuación se muestra las pruebas realizadas con diferentes comandos en los cuales demostramos todas las bondades implementadas gracias a la tecnología WPA:

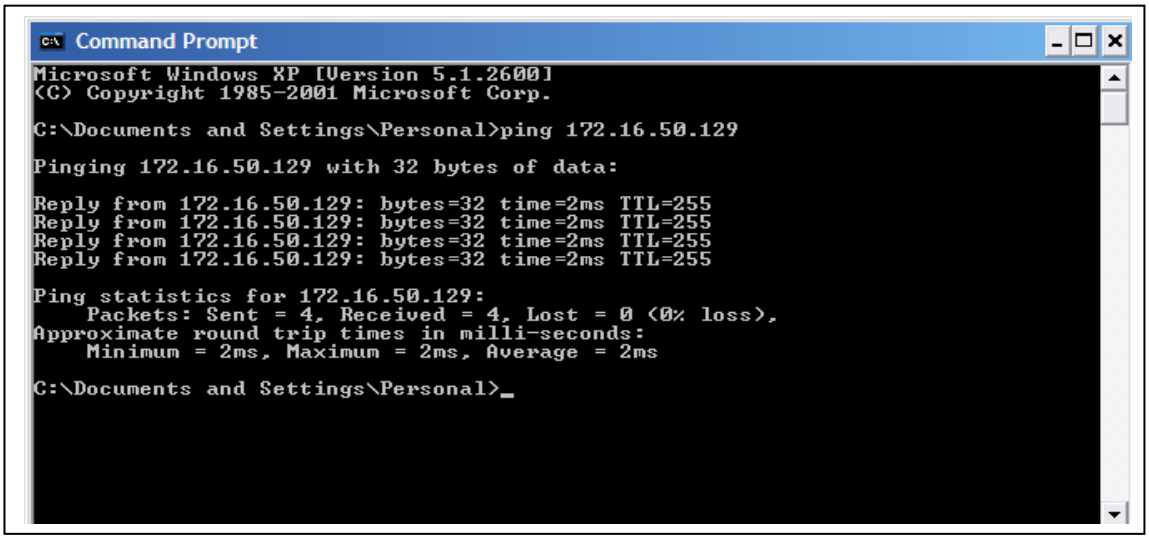
Al ejecutar este comando ipconfig/all se puede dar cuenta que la red inalámbrica se encuentra en perfecto funcionamiento, también se destaca las respectivas características

GRAFICO 3.6: EJECUCION DEL IPCONFIG/ALL UTC
FUENTE: GRUPO INVESTIGADOR.



También se puede mandar a ejecutar haciendo ping el número de la IP en este caso la 172.16.50.129 que es el ping asignado para comprobar que ya se encuentra conectado al puerto de salida del servidor, aclarando que solo el Director de Servicios Informáticos tiene esta clave secreta creada por la Migración WPA y el será el encargado de facilitar esta contraseña de acceso a la red inalámbrica a personas de su absoluta confianza como son los administradores de la misma.

GRAFICO 3.7: EJECUCION DEL PING UTC
FUENTE: GRUPO INVESTIGADOR.



3.1.2. Factibilidad Económica.

Al tratarse de seguridades en redes inalámbricas siempre puede sonar a gastos extremadamente fuertes, pero al tener la universidad instalado equipos de ultima generación y en algunos casos configurables como son los casos de los switch de CORE los mismos que permitieron clasificarlos en VLAN(Virtual Local Área Network), a las redes y de esta manera independizar su utilización, las antenas con que cuentan la Universidad son de igual manera las mejores del mercado fueron fabricadas por la

empresa 3com la misma que abasteció completamente de tecnología de telecomunicaciones a la Universidad.

Al contar con todo implementado nuestro trabajo y el de los administradores de la Dirección de Servicios Informáticos fue de otorgar una VLAN y configurar en el equipo Switch Inalámbrico los puertos y protocolos que va a servir de enlace entre los servidores y los usuarios de la red, cabe recalcar que la dirección para la red inalámbrica esta siendo administrada por el DHCP.

3.1.2.1. Función del DHCP (Dynamic Host Configuration Protocol)

El Protocolo de Configuración de Anfitrión Dinámico es utilizado Por que la red de la Universidad es amplia. El daemon actúa dándole información de la red a la estación de trabajo, tales como IP Address, Subnet Mask, DNS Server, Gateway, etc. Al igual que otros protocolos similares, utiliza el paradigma cliente-servidor, para que los nodos clientes obtengan su configuración del nodo servidor.

El protocolo de Configuración Dinámica de Hosts (DHCP) permite la transmisión de la configuración de los hosts sobre la red TCP/IP. Este protocolo se encarga de la configuración automática de los parámetros de red, utilizando direcciones. DHCP es una extensión de BOOTP, es decir, mejora BOOTP, y es compatible con él (un usuario puede realizar una petición estática BOOTP a un servidor DHCP).

DHCP es un protocolo que permite asignar direcciones IP dinámicas, de forma totalmente automática. Por ello no pierde las prestaciones de BOOTP, su predecesor, sino que las amplía permitiendo nuevas formas de asignación de direcciones y nuevas opciones para poder pasar a los clientes toda la información necesaria. DHCP es un protocolo implementado en los principales sistemas operativos así como otros dispositivos. DHCP puede usarse cuando el número de IPs es menor que el número de computadores y todos no están conectados a la vez, como en el proveedor de servicio de

Internet (ISP). El DHCP en la Universidad Técnica de Cotopaxi está formado por dos partes: un protocolo para el intercambio de los parámetros de red específicos de cada host y un mecanismo para la asignación de direcciones de red.

El servidor DHCP tiene dos bases de datos. La primera es estática, al igual que BOOTP y la segunda contiene una pila de direcciones IP disponibles. Esta segunda base de datos hace a DHCP dinámico. Cuando el usuario DHCP pide una dirección IP temporal, DHCP la coge de la pila de direcciones IP disponibles y se la asigna durante un periodo de tiempo negociado.

El intervalo está dado en la sub red:

172.16.50. XXX
255.255.255.192

3.1.3. Factibilidad Operacional.

La configuración de las seguridades fue desarrollado por el grupo investigador bajo supervisión y ayuda de los señores Ingenieros Miguel Cerda en calidad de Director y del Ing. Guido Segovia en calidad de Administrador de Aplicaciones WEB y Redes de Telecomunicaciones. Se hace urgente la implementación de nuevas antenas para la cobertura en el edificio antiguo ya que de esta manera garantizaríamos que el recurso como lo es el Internet vaya a todos los estamentos universitarios.

3.2. Distribución de Equipos de la Red Inalámbrica del Campus San Felipe

3.2.1. Antenas

Hoy en día se suelen utilizarse antenas parabólicas, para conexiones a larga distancia, también se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Entre los modelos y variantes de antenas, se pueden distinguir 2 grandes familias: Las antenas Direccionales y las antenas Omnidireccionales. Como su nombre indica, las direccionales emiten la señal hacia un punto en concreto, con mayor o menor precisión. Las "Omni" por el contrario, emiten por igual en todas direcciones, en un radio de 360, pero solo sobre el plano.

Dentro del grupo de antenas direccionales, tenemos las de Rejilla o Grid, las Yagi, las parabólicas, las "Pringles" las de Panel y las Sectoriales. Las omnidireccionales suelen ser una simple varilla vertical, aunque tienen su tela también hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias podremos cubrir con una antena, y con mejor calidad podremos captar señales que pudieran llegarnos muy débilmente ver Anexos.

- Antena de Parrilla de 24dB de ganancia: 70,5 Km. (El enlace entre Gran Canaria y Tenerife se hizo con ésta antena.)
- Antena de Parrilla de 19dB de ganancia: 54 km. entre dos antenas iguales.
- Antena Omnidireccional de 8dB de ganancia: 25 km. de distancia, al otro extremo había una de 19dB Grid. A 10km el enlace era a11Mbps, y a esa misma distancia conectamos entre 2 Omnis a 2Mbps.

Estas distancias se consiguieron gracias a condiciones MUY especiales, realmente excelentes. No son aplicables a trabajar en producción de forma permanente.

GRAFICO 3.8: ANTENAS PARABOLICAS UTC
FUENTE: www.wirelesslan.com

3.2.2. Switch Inalámbricos.

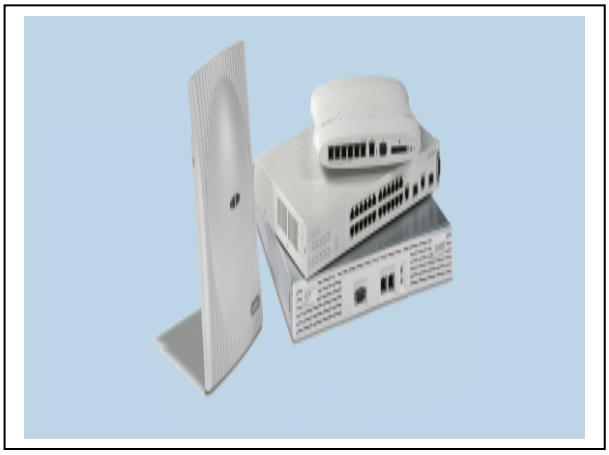
El Switch inalámbrico WS2000 es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en instituciones. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión. La compatibilidad con extensiones Wi-Fi Multimedia (WMM) permite al WS2000 ofrecer el mejor rendimiento incluso en las aplicaciones más complejas con voz y vídeo. El WS2000 ofrece tal nivel de sencillez y flexibilidad de gestión que elimina la necesidad y los costes de personal dedicado de TI en el sitio para gestionar las redes inalámbricas Ver Anexos.

- Lan inalámbrica: Admite 8 WLAN; AP virtual: segmentación de tráfico multi-ESS/BSSID; roaming preferente; equilibrio de cargas automático.
- Radio de puertos de acceso: Admite 1-6 puertos de acceso 802.11a/b/g; adopción acceso: automática de puerto de acceso con ACL; capacidad de selección automática de canales.
- Filtrado de paquetes: Análisis de paquetes de estado L2/3/4; traducción de direcciones de red (NAT).
- Gestión: Interfaz de línea de comandos (serie, Telnet, SSH); autenticación admin. a través de servidor Radius; Java Applet (HTTP, HTTP seguro); Syslog; archivos de configuración en formato de texto; configuración remota y actualizaciones de firmware (por TFTP, FTP); actualizaciones automáticas de

configuración y firmware mediante opciones DHCP; SNMP v1/v2/v3; MIBs MIB-II, Ping MIB, TraceRoute MIB, Symbol MIB.

- Interfases físicas: 1 puerto serial RS232 de consola. 7 puertos Ethernet 10/100 (incluido un puerto de enlace activo WAN). 4 puertos 802.3af compatibles con Power-over-Ethernet. Tarjeta CF (para almacenamiento).

GRAFICO 3.9: SWITCH INALAMBRICO UTC
FUENTE: www.wirelesslan.com



3.2.3. Access Point

Un Access Point es diseñado para actuar como el equivalente inalámbrico de un hub o switch ethernet. Permite que varios usuarios con equipos inalámbricos estén conectados a un hub central en el Modo Infraestructura (BSS). Esto significa, desde el punto de vista de una red cableada, que la red formada tiene forma de estrella. Cada cliente wireless habla con los demás a través del Access Point.

Los Access Point que usamos en el bloque B y C del campus San Felipe de la Universidad Técnica de Cotopaxi para el correcto funcionamiento de las redes inalámbricas wireless se encuentran estructurados como se puede ver en anexos, además de su respectiva distribución de equipos y computadoras.

Aparte de los Access Point comerciales, existen proyectos para poder usar un ordenador Linux o BSD en modo Access Point. El problema es que hay que tener un conocimiento muy elevado del modo de funcionamiento de las tarjetas wireless y los fabricantes no facilitan la tarea. El proyecto de Host-AP, que es esto de hacer funcionar una tarjeta normal conectada a un ordenador como Access Point tiene su sede aquí, pero actualmente solo se puede hacer con las tarjetas que posean el chip Prism2. Este es un mini Howto de la prism2 en modo Access Point.

TABLA 3.1: **CARACTERISTICAS DEL ACCES POINT UTC**.
FUENTE: **DIRECCION DE SERVICIOS INFORMATICOS**

Componente	**Características**
Descripción del producto :	NETGEAR WG102 ProSafe Wireless Access Point - punto de acceso inalámbrico
Tipo de dispositivo:	Punto de acceso inalámbrico
Tipo incluido :	Externo
Dimensiones (Ancho x Profundidad x Altura) :	14.1 cm x 10 cm x 2.7 cm
Peso :	0.4 kg
Protocolo de interconexión de datos :	IEEE 802.11b, IEEE 802.11g
Protocolo de gestión remota :	SNMP, Telnet, HTTP
Características :	Alimentación mediante Ethernet (PoE), enlace ascendente automático, filtrado de dirección MAC, pasarela VPN
Sistema operativo requerido :	Microsoft Windows 98/ME/2000/XP

3.2.4. Tarjetas de Red Inalámbricas.

Tarjeta de red inalámbrica para ranura PCMCIA Es aquella que permite conexiones de red inalámbrica entre el computador portátil y otros equipos con red inalámbrica. Totalmente compatible con el estándar 802.11g y 802.11b, proporciona comunicación inalámbrica de alta velocidad hasta 54 Mb a equipos portátiles con Windows 98Se, Me,

y XP. La tarjeta incorpora una antena integrada en su parte externa, proporcionando gran cobertura y alcance. Soporta encriptación de 64/128 bit WAP que garantizan la seguridad y privacidad de los datos enviados. Incorpora modo de ahorro de energía en el modo infraestructura para reducir al mínimo el consumo de energía del equipo.

GRAFICO 3.10: TARJETA IANLAMBRICA EN LA UTC
FUENTE: WWW.SUPERINVENTOS.COM

3.2.4.1 Adaptador PCI Red Inalámbrica Wi-Fi de 54 m/bits

El adaptador de red inalámbrico DWL-G520 es una tarjeta PCI a 32 bits que puede instalarse rápida y fácilmente en un PC permitiendo conectar con una red inalámbrica que cumpla con la norma 802.11b o 802.11g. Estos adaptadores inalámbricos pueden utilizarse en modalidad punto a punto o como interfaz de red normal. Ahora puede crear una red inalámbrica sin necesidad de instalar ni un solo cable. Por fin puede compartir su conexión de Internet con los demás usuarios de la Universidad Técnica De Cotopaxi. Conéctese a Internet desde las canchas deportivas, el bar universitario, el salón o desde cualquier parte con este adaptador de red inalámbrico de 54 mbits pero con las respectivas contraseñas de seguridad generadas por la Seguridad WPA.. Comparta datos, juegue en red o simplemente diviértase de forma totalmente segura gracias a su

encriptado de 256 bits. Compatible con redes de 54, 22 ,11 mbs o menos y redes wi-fi. Alcance en interiores hasta 100 metros y 100-150 en exteriores. Compatible con Windows 98, Me, 200 y XP.

El adaptador D-Link AirPlus Xtreme G DWL-G520 es una tarjeta de red diseñada para un bus PCI 2.2, con frecuencia de trabajo de 2.4GHz, compatible con el estándar 802.11g, que proporciona un ancho de banda de hasta 54Mbps. Dotada de la función plug-n-play, la tarjeta es fácilmente instalable en cualquier ordenador PC de sobremesa.

3.2.4.1.1 Aplicaciones

Entre las aplicaciones mas corrientes están la de conectar un equipo de sobremesa con otros equipos de la red sin necesidad de instalar cables. Esto puede resultar especialmente útil en instalaciones no permanentes como casa abiertas, congresos, demostraciones, foros, defensas de tesis, etc. Otra aplicación muy usual es cuando se quiere compartir la conexión de Internet de banda ancha con otros miembros de la familia y no es posible o deseable instalar cables con todo lo que ello significa.

TABLA 3.2: **ESPECIFICACIONES TECNICAS DE LA TARJETA INALAMBRICA** BLOQUES B Y C
FUENTE: **DIRECCION DE SERVICIOS INFORMATICOS**

Estándar	- IEEE 802.11 - IEEE 802.11b - IEEE 802.11g-Draft
Tipo de tarjeta	- PCI 2.2 32 bits
Transmisión de datos	- 54Mbps - 48Mbps - 36Mbps - 24Mbps - 18Mbps - 12Mbps - 11Mbps - 9Mbps - 6Mbs - 5.5Mbps - 2Mbps - 1Mbps

Cifrado WEP	- 64 bits - 128 bits - WPA -- Wi-Fi Protected Access (64-, 128-WEP con TKIP, MIC, IV Expansion, Shared Key Authentication)
Control de Acceso a Medios	- CSMA/CA con ACK
Frecuencia de Trabajo	- desde 2.4GHz hasta 2.4835GHz
Alcance señal	- Interiores: hasta 100 metros - Exteriores: 100 – 300 metros
Tecnologías de modulación	-- OFDM (Orthogonal Frequency Division Multiplexing) - CCK (Complementary Code Keying)
Sensibilidad del Receptor	- 54 Mbps OFDM, 10% PER, -68 dBm - 48 Mbps OFDM, 10% PER, -68 dBm - 36 Mbps OFDM, 10% PER, -75 dBm - 24 Mbps OFDM, 10% PER, -79 dBm - 18 Mbps OFDM, 10% PER, -82 dBm - 12 Mbps OFDM, 10% PER, -84 dBm - 11 Mbps CCK, 8% PER, -82 dBm - 9 Mbps OFDM, 10% PER, -87 dBm - 6 Mbps OFDM, 10% PER, -88 dBm - 5.5 Mbps CCK, 8% PER, -85 dBm - 2 Mbps QPSK, 8% PER, -86 dBm - 1 Mbps BPSK, 8% PER, -89 dBm
Potencia de salida	- 15dBm (32mW) ± 2dB
Antena	- Externa desmontable, conector SMA hembra
Temperatura de funcionamiento	- 0°C ~ 55°C
Humedad	- 95% máx. (sin condensación)
Dimensiones	133 x 121 x 18 mm
Peso	77 g.

3.3. Asignación de IP de acuerdo a disponibilidad de equipos con tecnología inalámbrica.

La tecnología inalámbrica por su flexibilidad debe trabajar directamente con los DHCP los mismos que ayudan a que los usuarios de computadores puedan adquirir una dirección IP de forma dinámica y esta a su vez pueda ser utilizada por cualquier persona

que invoque a la red, lo que si se debe procurar es tener una buena administración y control de asignación de IP ya que el rango es de cuando menos 240 equipos y el ancho de banda no justifica para ese numero.

3.4. Asignación de flujo de tráfico en Internet de acuerdo a perfiles.

Los perfiles están dados únicamente para el uso de algunas aplicaciones, pero aun no se tiene contemplado es la implementación de la red inalámbrica por lo que se convierte en un problema que debe ser tomado en cuenta ya que de parte de las autoridades, también posen equipos portátiles y al navegar por Internet sin encriptación podrían estos ser presa fácil de usuarios maliciosos.

3.5. Asignación de Ancho de Banda de acuerdo al número de usuarios

Seria lo ideal, otorgar un buen ancho de banda para cada una de las VLAN pero por lo limitado que es el recurso de Internet no podría ser dable, la intención del presente trabajo fue realizarlo sobre un ancho de banda de Internet que supere cuando menos el 1024 KBPS pero por tema de costos no fue posible por lo que se planifico restringir el uso del Internet inalámbrico a velocidades no mayores a 56 KBPS a cualquier hora del día.

3.6. Controlar de manera eficiente el acceso a la red inalámbrica de parte de los usuarios

3.6.1 WPA como medio de difusión en la Universidad Técnica de Cotopaxi

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

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse. En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo el usuario de un sistema identificados con nombre/contraseña o la posesión de un certificado digital.

Hoy en día mantener una buena seguridad dentro de una red inalámbrica es sin duda fundamental para la Universidad Técnica de Cotopaxi, así como en otras instituciones del país. Estos riesgos aparecen en el momento en que la información fluye libremente por el aire, siendo susceptible de ser examinada incluso fuera de los Bloques B y C donde está ubicada la red o bien de ser afectada por interferencias.

Los intrusos informáticos están a la orden del día y han ocasionado perdidas grandiosas a la Universidad a través del robo de Internet en forma ilegal así como de información confidencial en la misma. Las redes de computadoras y cualquier información en la Web se dice que no es segura y mas aun si hablamos de redes inalámbricas en donde si nuestra instalación no esta segura por medio de cualquier mecanismos actualizado como el WPA que lo implantamos, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo donde podríamos tener carpetas compartidas o analizar toda la información que viaja por nuestra red inalámbrica del campus.
Es por ello que La Universidad Técnica de Cotopaxi esta utilizando actualmente protocolos de autentificación de usuarios como es el WEP los cuales no garantizan una seguridad absoluta pero si al menos un buen apoyo para nuestra red. Y justamente el protocolo WPA (Wi-Fi Protected Access) que viene integrado en la mayoría de los dispositivos inalámbricos con el certificado Wi-Fi como lo son routers o Access point

que nos proporcionan nuestros proveedores de Internet, tratara de darnos la mayor seguridad posible a la red inalámbrica de la Institución.

Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un usuario se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, para permitir el tráfico de validación entre el usuario y una máquina de la de local. Una vez que se ha validado a un usuario es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los usuarios WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS que describimos más adelante.

WPA utiliza TKIP TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

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

3.7. Controlar la validación para la utilización de recursos de red inalámbrica

Las seguridades que disponen las antenas que se encuentran implementadas en la Universidad nos obligo a asignar contraseñas de encriptación independientes para no alterar el normal funcionamiento de la red inalámbrica de los bloques B y C, y que la información pueda fluir de una manera mas optima, cabe recalcar que las VLAN son las mismas para cualquiera de los dos bloques académicos lo que el ancho de banda es el mismo en donde uno se desee conectar.

CAPITULO IV

3.8. Conclusiones

1. La carencia de dispositivos de cobertura inalámbrica como switch y Access Point, en uno de los edificios, hace que la cobertura no abastezca al edificio antiguo ya que tiene algunas interferencias que hace que el servicio de red no sea el adecuado y se produzca retarde en las respuestas a las peticiones que realizan los usuarios de la red inalámbrica.

2. La aplicación de normas de seguridad, permite a los administradores de la red tomar el control de los riesgos a los que puede estar sujeta la red inalámbrica y de esa manera asegurar el rendimiento de la red tanto en el Bloque B como en el C del Campus San Felipe.

3. Con el avance tecnológico a permitido notablemente la reestructuración de los diferentes estándares de la IEEE y dentro de estos se ha implementado la seguridad inalámbrica mediante los estándares 802.11 b y g.

4. El estándar IEEE 802.11 define mecanismos que permiten a múltiples redes inalámbricas compartir adecuadamente un mismo medio físico sin que esto implique ningún tipo de interferencias entre redes y que gatrantize el flujo de la información.

5. La seguridad WEP implantada en la Universidad es demasiado frágil, causando demasiadas interferencias a los usuarios y no garantizando el flujo de información lo cual motivo a la implementación de la tecnología WPA.

6. Al tener una interconexión inalámbrica debe existir seguridades para cuidar la carga de la red ya que al tener solamente 512 KBPS de ancho de banda en la conexión a Internet de forma simétrica resulta que no abastece para el numero de estudiantes que tiene la institución y el numero de investigadores que utilizan este recurso en horas pico.

7. Al no existir la documentación necesaria y confiable de la distribución de la red inalámbrica los administradores de la misma, al momento de existir un inconveniente no podrán detectar en donde se produjeron fallas.

8. Con la realización de este proyecto de grado se ha identificado cuales son las falencias que tiene la red inalámbrica en cuestiones de seguridad, con el cuál los administradores podrán tomar las decisiones necesarias para brindar un mejor servicio a los usuarios.

9. La Dirección de Servicios Informáticos con la aplicación de este proyecto de grado garantizara que la información que circula por la red de la Universidad, Campus San Felipe tendrá la calidad de servicio necesaria en beneficio de cada uno de los usuarios al momento de recibir la información.

3.9. Recomendaciones

1. Es necesario la implementación de switch y Access Point en la red inalámbrica de uno de los edificios para de esa manera evitar las interferencias, que son las causantes de los retardes en las peticiones que hacen los usuarios.

2. Es necesario que las normas de seguridad implantadas mediante los estándares sean aplicadas correctamente por parte de los administradores que deben tomar el control de la red, de esta manera el servicio de la red inalámbrica será el más adecuado y obtendrá respuestas inmediatas a las peticiones que realizan los usuarios de la misma.

3. Los estándares 802.11 b y g estudiados en este proyecto de tesis están en constante actualización por lo que es necesario no dejar de lado dichas actualizaciones y aplicarlas en la Universidad para mejorar el servicio a cada uno de los usuarios.

4. La manera eficaz de evitar conflictos de seguridad en la red inalámbrica de la institución es aplicar correctamente la tecnología WPA que se ha implementado, y seguir con este proceso de cambio con tecnologías que saldrán al mercado a futuro.

5. Es necesario cuidar la carga de la red inalámbrica por el nivel limitado al que se ajusta el ancho de banda de la red en la conexión al Internet, para poder compartir la información en tiempo real y garantizar el verdadero flujo de la información en cualquier lugar dentro de la Institución.

6. Se recomienda que todos los laboratorios de la Universidad Técnica de Cotopaxi estén sujetos bajo las normas de estandarización de seguridades de redes inalámbricas para de esa manera ofrecer un servicio de calidad a los usuarios de la red.

3.10. Glosario de términos y siglas

Access Point

Es un producto comercial diseñado para actuar como el equivalente inalámbrico de un hub o switch ethernet. Permite a varios clientes inalámbricos conectados en un hub central en el Modo infraestructura (BSS).

Ad Hoc

La red Ad Hoc consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales Wi-Fi sin usar un punto de acceso.

Bluetooth

Tecnología de comunicación inalámbrica que permite la conexión entre diferentes equipos en un corto alcance (máx. 10 mts, opcionalmente 100m con repetidores y dependiendo de la clase) vía radio sin necesidad de estar unidos físicamente.

BSS

Infraestructura o BSS, aquí si es necesario el punto de acceso, que es quien centraliza la información, los PC se conectarán todos al mismo punto de acceso.

DHCP

DHCP: Dynamic Host Configuration Protocol. Un protocolo TCP/IP que asigna dinámicamente una dirección IP a un ordenador.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

EAP

Definido en la RFC 2284 [11], es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS.

ESS

Es una configuración que permite unir varios puntos de acceso, es decir, una red ESS está formada por varias redes BSS.

ESSID

Es un identificador de red inalámbrica. Es algo así como el nombre de la red, pero a nivel WIFI.

Ethernet

Ethernet se estandariza como IEEE 802.3. Ethernet es el estándar de LAN implementado más común. Admite velocidades de transferencia de datos de Mpbs, compatibles con velocidades de 10, 100 ó 1000 Mbps.

HACKER

Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.

Hub

Un hub de red es como el eje de la misma. Une las líneas de comunicación en un único lugar, ofreciendo una conexión común para todos los equipos y dispositivos de su red.

IEEE

Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicación y redes.

IEEE 802.11b

El estándar **IEEE 802.11b**, conocido también como "Wi-Fi" o como "Wireless Ethernet", define los niveles físico y de acceso al medio (MAC) El acceso al medio se basa en un mecanismo de contienda similar al de Ethernet.

IEEE 802.11g

La versión **IEEE 802.11g** puede alcanzar la misma velocidad máxima que 802.11a pero usando la misma banda de 2,4 GHz que 802.11b con dos opciones: OFDM o DSSS mejorado. Entre las ventajas de esta versión cabe citar la compatibilidad con 802.11b y un mayor alcance esperado debido a combinar las ventajas de OFDM en cuanto a multitrayecto con la menor absorción de la banda de 2,4 GHz.

IrDA

Siglas de "Infrared Data Association", Empresa que da nombre a los puertos IrDA, que permiten la comunicación sin cables entre dos dispositivos a través de rayos infrarrojos, la tasa de transferencia de datos es similar a la de un puerto paralelo, se requiere que los dos dispositivos se vean.

ISO/IEC

ISO/IEC 17799 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

MIC

MIC (*Message Integrity Code*). Código que verifica la integridad de los datos de las tramas.

Proxy Server

Un Server que se sitúa entre la aplicación cliente, como por ejemplo un web browser, y un Server real. Intercepta todos los requerimientos al Server real para ver si las puede resolver él. Si no, envía el requerimiento al Server real. Los Proxy Server tienen dos propósitos principales.

RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autentificación y autorización para aplicaciones de seguridades en redes inalámbricas.

Router

Dispositivo que conecta redes separadas. Los routers reenvían paquetes entre dos o más redes. Los routers funcionan al nivel de la Capa 3.

SSID

El SSID (Service Set IDentifier) es una clave alfanumérica de 32 caracteres que identifica exclusivamente a una LAN inalámbrica. A menudo se le refiere como el "Nombre de Red". Es utilizado para prevenir el acceso a su LAN de equipos inalámbricos no autorizados.

Switch Inalámbrico

El Switch inalámbrico es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en sucursales. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión.

TKIP

TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama, utiliza claves de sesión dinámicas de 128 bits, para cada usuario, cada sesión y cada paquete.

TCP:

Transmission Control Protocol. Protocolo de control de Transmisión. Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

VLANs

Las LANs virtuales (VLANs) son agrupaciones de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus.

VPN

Las **VPN** es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WECA

WECA (Wireless Ethernet Compatibility Alliance), es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse Wi-Fi Alliance.

3.11. Bibliografía

RODRÍGUEZ, JORGE (1999); Introducción a las Redes de Área Local; Editorial McGraw-Hill; México.

TENEMBAUM ANDREW S. (1999); Sistemas Operativos Distribuidos; Editorial Prentice Hall; México.

CARBALLAR, JOSÉ A. (2006); El libro de las Comunicaciones del PC, HP, Editorial Madrid MCGraw Hill, España.

MOREIRA, ADRIANO C. (2002); DOCUMENTO IEEE "Redes Híbridas"; Universidad de Averió; Portugal.

PERKINS, CHARLES E. (2003); Seguridad en Redes Inalámbricas; Editorial McGraw-Hall; Madrid.

KONSTANTIN GAVRILENKO (2005), Hacking Wireless, Editorial GRUPO AMAYA S.A, Madrid.

MIKHAILOVSKY ANDREI A. (2005); El mundo de la Seguridad Inalámbrica; Ediciones AMAYA S.A, Madrid.

VLADIMIROV ANDREW A.(2005), Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.

ANSI/IEEE Std 802.11, 1999 Edition."Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"

Hills. "Large-Scale Wireless LAN Design". IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

3.11.1 Web Bibliografia

- http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridadenredesinalambricas WiFi.shtml
- http://standards.ieee.org/getieee802/portfolio.html

- http://standards.ieee.org/getieee802/802.11.html
- http://www.wi-fi.org/OpenSection/secure.asp?TID=2
- http://www.microsoft.com/latam/prensa/2003/mar/wi-fi_protected_access.asp
- http://www.microsoft.com/spain/seguridad/guidance/topics/cryptographyetc.msp
- http://www.pucelawireless.net/index.php?pagename=AccessPoint
- http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml.
- http://www.virusprot.com/cursos/Redes-Inal%C3%A1mbricas-Curso-gratis17.htm
- http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml
- http://es.wikipedia.org/wiki/Red_privada_virtual#Conexi.C3.B3n_de_Acceso_Remot.
- http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_5708.html