UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

CARRERA DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TITULO:

"Construcción de un Punto de Acceso (AP) mediante una computadora personal utilizando GNU/Linux para administrar recursos como servidor de archivos, internet y firewall"

Tesis presentada previa a la obtención del título de Ingeniero en informática y sistemas Computacionales

AUTORA:

Herrera Herrera Tania Yahaira

.

DIRECTOR DE TESIS:

ING. PATRICIO NAVAS MOYA.

LATACUNGA - ECUADOR

Octubre – 2010

PAGINA DE RESPONSABILIDAD DE AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de su autora, egresada: Tania Yahaira Herrera Herrera

…….

Tania Herrera H.

050273670-5

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que la postulante: Herrera Herrera Tania Yahaira, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "Construcción de un Punto de Acceso (AP) mediante una computadora personal utilizando GNU/Linux para administrar recursos como servidor de archivos, internet y firewall", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 13 de Octubre del 2010

Atentamente,

Ing. Patricio Navas Moya.
DIRECTOR DE TESIS

AGRADECIMENTO

Agradezco primeramente a Dios y a todas aquellas personas que con su apoyo me ayudaron a conseguir mis metas de manera especial a mis hermanos: Ximena, Richard, Josué, mis sobrinos: David, Alexis, Maite, Josué , Maybrith, a Edu que fue parte de mi escuela en mi hogar, a Gladyz Castro y Ramiro Villarroel mis padres que siempre están apoyándome con sus consejos y amor, a María Eliza, María Belén mis hermanitas queridas, a mis cuñados y amigos Patty Álvarez y Juan Jiménez a mi amiga Norma, a mis abuelitos Rosita y Segundo, a mis Profesores que impartieron sus conocimientos, al Ing. Patricio Navas que a más de ayudarme con sus conocimientos fue mi guía y amigo para poder hacer que este proyecto llegue a su fin, y a todas aquellas personas que me de una u otra manera están a mi lado y me apoyan. Además agradezco infinitamente Universidad Técnica de Cotopaxi por haberme abierto las puertas para formarme como una mujer de bien.

DEDICATORIA

El presente proyecto se lo dedico a Dios a mi Mami María por ser Madre y Padre conmigo, a mi amado Hijo Eitan Fernando a mi Esposo Wilson, a ellos por el constante apoyo, valores, amor y cariño que me han brindado por la confianza y paciencia depositada para que este sueño llegue a ser una realidad, también quiero dedicarlo a esa persona especial que por algún motivo no estuvo a mi lado, que en algún lugar del cielo me está mirando y enviando sus bendiciones.

Tania Yahaira

ÍNDICE GENERAL

INTRODUCCIÓN

En los últimos tiempos la informática es la herramienta más poderosa que el hombre ha tenido en sus manos y que en este momento interviene de forma directa o indirecta en, prácticamente, todas las actividades humanas. Dejar que esta herramienta sea controlada y restringida por agentes solo interesados en su propio lucro supone un perjuicio para las sociedades. La interconectividad inalámbrica constituye una oportunidad histórica de tomar el control de nuestro propio destino. Por esta razón es hora ya que empresas, instituciones, universidad y hogares hagamos conciencia, y busquemos la manera de explotar de mejor manera este recurso.

Desde siempre el anhelo de todos los usuarios de computadores personales o de portátiles, ha sido el poder contar con el Internet en todo su hogar u oficina sin necesidad de estar relegado a un solo sitio, pudiendo movilizarse a través de toda la casa o de todas las oficinas que pueden constituir una institución o empresa. Como consecuencia de esto todos buscamos alternativas para lograr alcanzar y cumplir con esta meta.

La mejor manera de alcanzar este objetivo es equipar las computadoras de la oficina y las portátiles con trasmisores y receptores de radio de onda corta que permita comunicarse. Todo esto hizo que más empresas busquen comercializar las redes inalámbricas, para satisfacer las necesidades de comunicación tanto a clientes como instituciones.

En la Universidad Técnica de Cotopaxi a partir de la construcción del Bloque Académico B de Ciencias de la ingeniería y Aplicadas se decide adoptar está tecnología luego de un minucioso estudio de factibilidad en la cual se investiga marcas y desempeño de cada una de ellas, se revisó, las prestaciones alcance, versatilidad y por supuesto la escalabilidad, es necesario manifestar que aquí se adoptó a 3com como alternativa de conexión inalámbrica con un gran concentrador que es una antena.

El objetivo del presente tema de estudio fue demostrar que mediante una computadora personal se puede obtener un concentrador o punto de acceso para administrar redes

inalámbricas y además de que con este servicio podremos brindar un buen servicio de intercomunicación entre computadoras, adicionalmente flexibilidad para el traslado de los computadores de un lado a otro, adicionando un valor agregado que es la seguridad de la información, precautelando las actividades de los usuarios de red.

De las fortalezas de la presente investigación es el poder contar con suficiente información bibliográfica, además de que se basó íntegramente en los estándares internacionales para las configuraciones, como fue el caso del estándar de la IEEE 802.11b y g y por otro lado debemos mencionar la gran ayuda prestada de parte del personal de Servicios Informáticos y de los docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales que fueron de mucha ayuda para poder llegar a culminar con éxito está investigación.

Este trabajo de investigación para una mejor interpretación se lo ha estructurado en tres capítulos:

El primer capítulo corresponde a la descripción de algunos aspectos importantes de las redes Inalámbricas, de las WLAN (Wireless Local ÁREA Network), así como información de las Seguridades, servidores, etc.

El segundo corresponde a la investigación de campo, el mismo que estuvo planificado de acuerdo a las metodologías de la parte técnica tecnológica, así como también de las entrevistas al Director de la Dirección de Servicios Informáticos, al director de la Tesis como entes representativos dentro del Área Tecnológica de la Universidad, por ultimo comprobamos el cumplimiento de la Hipótesis planteado en el desarrollo del anteproyecto de Tesis.

El tercer capítulo consta las configuraciones para la elaboración del punto de acceso, del proxy para la repartición de calidad de servicio de internet, además de las seguridades de las redes inalámbricas, previo el estudio de la factibilidad técnica-tecnológica y económica.

Finalmente las conclusiones con sus respectivas recomendaciones producto del presente trabajo de investigación.

RESUMEN

En el contexto de las redes informáticas, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Está investigación se basa en la construcción de un Access Point el mismo que servirá como servidor proxy para poder gestionar de un manera adecuada las comunicaciones de cualquier institución, empresa en el propio hogar ya que no se requiere de mayor inversión que la configuración de un computador con un sistema operativo que tenga la capacidad de trabajar como servidor, se esté Windows o de código abierto como Linux en sus distintas versiones.

Las configuraciones se las realiza a nivel de DHCP para que pueda ofrecer a los clientes la asignación de direcciones IP de forma automática, se debe contar con un computador con al menos una tarjeta de red inalámbrica la misma que proveerá la señal, entre más alcance esta pueda tener se podrá ofrecer un mejor servicio, las características deben ser las más básicas ya que este computador estaría dedicado solamente a esta actividad es decir a proveer servicio de proxy a los clientes de una red inalámbrica.

La investigación se lo hace para ayudar a los estudiantes de la Universidad Técnica de Cotopaxi y de la Carrera de Ingeniería en Informática y Sistemas Computacionales para que puedan optimizar los recursos de una manera eficiente ya que esta investigación precisamente ayuda a explotar los computadores que fueron de generaciones anteriores a los que se utilizan hoy en día, aun cuando la tarjeta de red se necesita que tenga una muy buena cobertura para que está cubra una mayor área de influencia.

RESUME

In the computer network context the term “proxy” does reference of a dispositive or program that realize an action like showing of another one. The most habitual function is of the user “proxy” which allows the access to the internet and all equipment’s of an organization when only we can dispose of a device connected, it is a definitive straight called IP.

This research is based in the construction of an “access point”. The same programmer which will be used as user “proxy” so we can control of an appropriate way the communication of whatever institution, company or in the own house because in doesn´t need of a huge investment, else the adapting of the computer with an operator´s system to be available for walking as user although this be of windows or the key open like “Linux” in its different designs.

The programmers are made in a level of “DHCP” so it can offer to the clients the assignment of direction IP in automatic way. It´s necessary have else a computer with unwire net which will provide the signal, if it has a major level can offer a best service.

The characteristic are the most appropriate because this computer world be only delicate at this activity, it is to provide service of “proxy “to the clients of a unicare net.

The research is done for helping to the Cotopaxi Technical University students of engineering career and computer system and informatics so they can improve the sources of an efficient way to due this research help to explode the oldest computer which belonged at before generations and nous day we use even when net´s card needs having a great signal to cover a major area of influence.

Latacunga, 15 de junio del 2010.

CERTIFICO:

A QUIEN LE INTERESE:

QUE LA SRTA. TANIA YAHAIRA HERRERA HERRERA CON C.I.# 0502736705, HA TRADUCIDO CORRECTAMENTE EL RSUMEN DE SU PROYECTO DE TESIS CON EL TEMA: **"CONSTRUCCION DE UN PUNTO DE ACCESO (AP) MEDIANTE UNA COMPUTADORA PERSONAL UTILIZANDO GNU/LINUX PARA ADMINISTRAR RECURSOS COMO SERVIDOR DE ARCHIVOS, INTERNET Y FEREWALL"** REALIZANDOSE EN LA UNIVERSIDAD TECNICA DE COTOPAXI, ES TODO LO QUE PUEDO DECIR EN CUENTO A LA VERDAD.

ATTE:

LIC. ROSARIO CEDEÑO
LICENCIADA EN EL IDIOMA INGLES.

CAPITULO I

1. CONECTIVIDAD INALÁMBRICA

1.1. REDES INALÁMBRICAS

1.1.1. Conceptos

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”.[1]

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

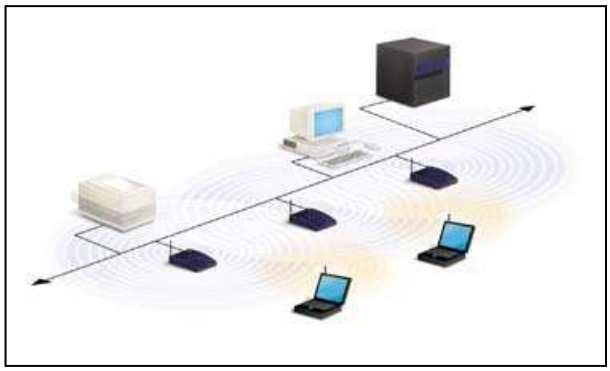


Gráfico 1.1: REDES INALAMBRICAS
Fuente: EL INVESTIGADOR

1.1.2. Orígenes

"Las redes de área local inalámbrica funcionan desde hace varios años en entornos industriales y de investigación.

Se implementaron por primera vez en 1979 como resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

En marzo de 1985 la Comisión Federal de Comunicaciones, FCC, organismo encargado de la regulación de las telecomunicaciones en Estados Unidos, asignó a los sistemas WLAN las bandas frecuenciales 902-928 MHz., 2.400-2.4835 GHz. y 5.725-5.850 GHz también conocidas como ISM (Industrial, Científica y Médica) y que pueden utilizarse bajo licencia administrativa.

Esta asignación de una localización frecuencial fija propició una mayor actividad industrial. En este punto las redes de área local inalámbrica dejaron de ser meramente experimentales para empezar a introducirse en el mercado.

Entre los años 1985 y 1990 se trabajó en el desarrollo de productos WLAN y finalmente, en mayo de 1991, se publicaron algunos trabajos que hablaban

sobre redes inalámbricas que superaban la velocidad de transferencia de 1 Mbps, velocidad mínima a partir de la cual el comité IEEE considera que una red es de área local.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y precios elevados de la solución inalámbrica". [2]

En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100 % anual. Este hecho es atribuible a dos razones principales:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles que han producido que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red. En este sentido, las comunicaciones inalámbricas ofrecen una prestación no disponible en las redes cableadas: movilidad y acceso simultáneo a los recursos de la red.

- La conclusión de la definición de la norma IEEE 802.11 para redes de área local inalámbricas el pasado junio de 1997 que ha establecido un punto de referencia y ha mejorado muchos de los aspectos de estas redes.

A pesar del atractivo y funcionalidad de las WLAN, la falta de estándares que brinden confianza a los potenciales usuarios de esta tecnología, fue otra de las razones de la lenta acogida que tuvieron en el pasado. En la actualidad se han definido normas internacionales que regulan la operación y funcionamiento de los elementos y protocolos de WLAN. Entre las normas más importantes para este tipo de redes tenemos la realizada por e! subcomité 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos de los Estados Unidos (IEEE).

[2] Tomado de: www.monografias.com/reporte/redesinal/redinal.htm

1.1.3. Ámbito de aplicación

En nuestra era han surgido los adictos a la información, gente que necesita estar todo el tiempo en línea. Para estos usuarios móviles, cable de par trenzado, el cable coaxial y la fibra óptica nos son útiles.

Ellos necesitan obtener datos para sus computadores laptops, notebook, de bolsillo, de mano, celulares, de pulsera o reloj, sin estar limitados a la infraestructura de comunicaciones terrestres. Para estos usuarios la comunicación inalámbrica en general veremos que tiene otras aplicaciones importantes además de proporcionar conectividad a los usuarios que desean navegar por la WEB.

1.1.3.1. 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."[3]

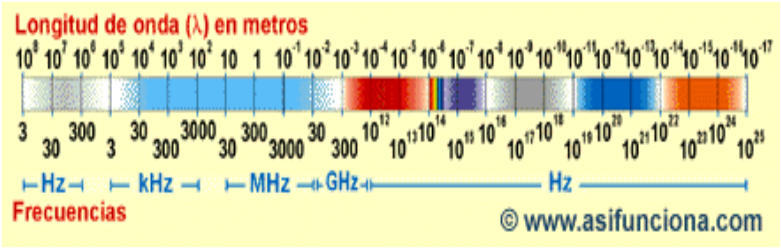


Gráfico 1.2: ESPECTRO ELECTROMAGNÉTICO.
Fuente: WIKIPEDIA, LA ENCICLOPEDIA LIBRE.

[3] Tomado de: www.wikipedia.org/ondas.html, Espectro Eletromagnético, Pablo Sanchez, Mayo 2006.

1.1.3.2. 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)"[4].

1.1.3.3. 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"[5].

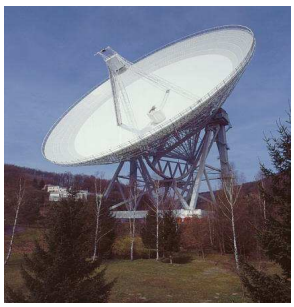


Gráfico 1.3: ONDAS DE RADIO
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

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

[4] Tomado de: www.wikipedia.org/ondaselectro.html, Ondas Electromagnéticas, Pablo Sanchez, Mayo 2006.
[5] Tomado de: Redes de Computadoras, Cuarta Edición, TANENBAUM Andrew, Editorial Prentice Hall, Año 2005, Pág. 65

necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

Gráfico 1.4: MICROONDAS TERRESTRES
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.1.3.4. 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.

1.1.3.5. 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 $7x10^{-7}$).

1.1.3.6. 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.

1.1.3.7. 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.

1.1.4. Wireless LAN entre oficinas

La tecnología WLAN puede remplazar a las redes cableadas tradicionales o ampliar su alcance y sus capacidades. De igual modo que sus homologas con cables, el equipo de las WLAN interiores se compone de una tarjeta PC y adaptadores de clientes PCI e ISA, así como de Puntos de Acceso, que realizan funciones similares a las que realizan los hubs en las redes tradicionales.

1.2. PROTOCOLOS DE TRANSMISIÓN

Los diversos mecanismos de acceso que se han propuesto e implantado para WLAN se agrupan en dos categorías: protocolos con arbitraje (FDMA, TOMA) y protocolos por contención (CDMA/CD, CDMA/CA).

Tipo de configuración WLAN sencilla, entre varias computadoras sin necesidad de usar un Access Point también se han diseñado protocolos que son una combinación de estas dos categorías.

Aunque ya no es habitual su utilización dentro de los sistemas WLAN, el mecanismo de mulitplexación en frecuencia, FDMA, divide todo el

ancho de banda asignado en distintos canales individuales. Este es un mecanismo simple que permite el acceso inmediato al canal, pero poco eficiente para su utilización en sistemas que presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa algo más factible es asignar todo el ancho de banda disponible a cada nodo durante un breve intervalo de tiempo de manera cíclica, este sistema llamado multiplicación en el tiempo (TOMA), requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias.

Este último esquema ha sido utilizado con cierto éxito, sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

Por el contrario, el protocolo de acceso múltiple por división de código (COMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes.

Varias de las primeras redes utilizaban el algoritmo de acceso al medio, CSMA/CD. El cual se caracteriza por comprobar previamente que el medio de comunicación esté libre, antes de iniciar la transmisión. Si se tiene esta condición, entonces se transmite la información y si no, se espera a que se libere el medio.

Como existía la posibilidad de que dos estaciones transmitieran información simultáneamente, este mecanismo exigía que a pesar de iniciar la transmisión se debiera continuar con la vigilancia del canal para detectar posibles colisiones. Cuando esto ocurría, la transmisión era suspendida y las estaciones involucradas en el conflicto debían esperar un tiempo aleatorio antes de repetir nuevamente el algoritmo.

El protocolo 802.11, utiliza un tipo de protocolo conocido como CSMA/CA (Carrier-Sense, Múltiple Access, Colusión Avoidance). Este protocolo introduce una variante en el algoritmo anterior que evita las colisiones en la transmisión, en lugar de descubrir una colisión, fundamentado en el hecho de que la mayor probabilidad de que se produzca una colisión en CSMA/CD se da al terminar una transmisión.

Es decir, al haber más de una estación esperando que una transmisión en curso termine para que ellas puedan comenzar a transmitir, si no se adoptan las medidas oportunas estas estaciones comenzarán, todas a la vez, a enviar información provocando una colisión en el medio.

En el sistema CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir, disminuyendo
así la probabilidad de colisión.

A pesar del buen comportamiento general de este sistema, presenta una deficiencia debida al problema conocido como Terminal Oculto. Este problema se presenta cuando un dispositivo inalámbrico transmite con la potencia justa para que sea escuchado por un nodo receptor, pero no con la suficiente como para que otra estación, que se encuentra a la espera, sepa que hay otra unidad que está transmitiendo. Para resolver este conflicto, se ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo.

Este proceso hace que cuando una estación está lista para transmitir, primero envía una solicitud al punto de acceso (RTS - Request to Send)) quien, si no encuentra problemas, responde con una autorización (CTS - Clear to Send) que permite al solicitante enviar su datos. Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK - acknowledgment packet) notificando al transmisor el éxito de la transmisión.

Independientemente de los protocolos de acceso al medio y para dar soporte a las medidas de seguridad tan necesarias en este tipo de redes, ios sistemas inalámbricos, como complemento adicional y característica optativa para evitar las escuchas indiscretas, disponen de una herramienta de codificación de la información. La seguridad de los datos se realiza mediante una compleja técnica de codificación conocida como WEP (Wired Equivalent Privacy Algorithm).

El sistema WEP se basa en proteger los datos transmitidos en el medio RF, usando una clave generada por un número pseudo aleatorio y un algoritmo de encriptación. Cuando se habilita este sistema, sólo se protege la información del paquete de datos y no protege el encabezamiento de la capa física para que las demás estaciones puedan escuchar el control de datos necesario para la adecuada gestión de la red.[6]

1.3. ORÍGENES DE LAS REDES DE ÁREA LOCAL 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 Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones,

[6] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 120-139

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.[7]

Gráfico 1.5: REDES WLAN
Fuente: WWW.AIRONET.COM

1.4. TIPOS DE REDES INALÁMBRICAS

1.4.1. 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

[7] www.aironet.com/wireless.php, Origen de la tecnología inalámbrica, Juan Paúl Salvatierra, Octubre 2003.

éxito de todos los 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.

1.4.2. Métodos de Acceso celular

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.

1.4.3. 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.

1.4.4. 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 cualquier lugar 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.

1.4.5. 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).

1.5. REDES PÚBLICAS DE RADIO

Las redes públicas tienen dos protagonistas principales: "ARDIS" (una asociación de Motorola e IBM) y "Rarn Mobüe Data" (desarrollado por Ericcson AB, denominado MOBITEX). Este último es el más utilizado en
Europa.

Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia.

La compañía proporciona la infraestructura de la red, se incluya controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software, por ejemplo una compañía llamada RF Data, desarrolló una rutina de compresión de datos para utilizarla en estas redes públicas).

Los fabricantes de equipos de cómputo venden periféricos para estas redes (IBM desarrolló su "PCRadio" para utilizarla con ARDIS y otras redes, públicas y privadas).

La PCRadio es un dispositivo manual con un microprocesador 80C186 que
corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de
memoria y 640 Kb de RAM.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta).

1.6. VENTAJAS DE LAS REDES INALÁMBRICAS

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

1.7. ESTÁNDARES INALÁMBRICOS

1.7.1. IEEE 802.11(A), IEEE 802.11(B), IEEE 802.11(G)

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

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.

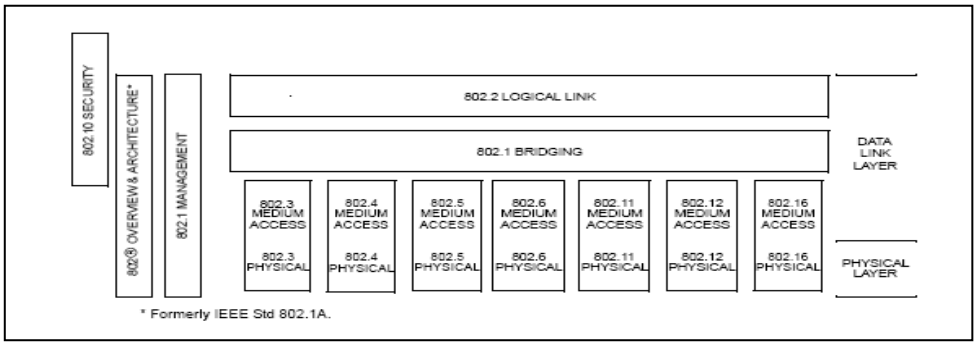


Gráfico 1.6: FAMILIA DE LOS ESTANDARES DE LA IEEE. 802.11

Fuente: http://www.ieee.org

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).

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.

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 e 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".[8]

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

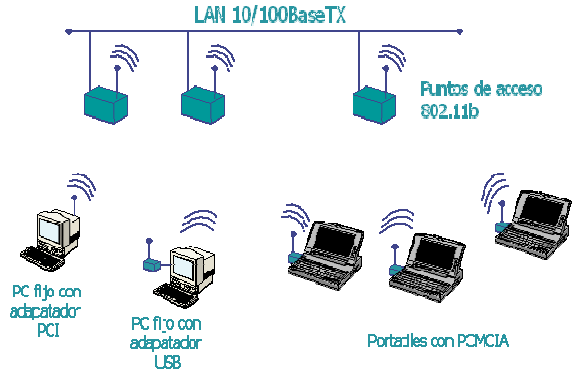


Gráfico 1.13: ESTANDARES DE CALIDAD PARA LAS REDES INALAMBRICAS

Fuente: EL INVESTIGADOR

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".

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.

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).

1.8. TOPOLOGÍAS Y PROTOCOLOS INALÁMBRICOS

1.8.1. Redes 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.

1.8.2. Redes de infraestructura

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.

1.9. INSTALACIÓN Y CONFIGURACIÓN DE ACCESS POINT

1.9.1. Modelos de operación

Hay dos modos de operación, uno ad-hoc, en el que las estaciones se comunican entre sí directamente, y otro de Infraestructura, en el que las estaciones acceden a la red a través de uno o varios puntos de acceso.

El interés suscitado en este campo de las redes inalámbricas ha posibilitado una rápida evolución del estándar inicial y actualmente existen tres extensiones:

- **802.11b** "Higher-Speed Physical Layer Extension in the 2.4 GHz Band".-
  - Estándar predominante de red inalámbrica en redes locales para la empresa y el hogar, así como puntos de conexión públicos.
  - Se ejecuta en tres canales en el espectro de los 2,4 GHz
  - Transfiere datos a velocidades de hasta 11 Mbps en distancias que alcanzan unos 90 metros.

- **802.11a** "High-speed Physical Layer in the 5 GHZ Band".

  - Se ejecuta en 12 canales en el espectro de los 5 GHz
  - Transfiere datos a velocidades de hasta 54 Mbps en distancias que alcanzan unos 15 metros.
  - No es compatible con 802.11 b, por lo que necesitará un nuevo equipo inalámbrico si cambia de estándar
  - Pocos problemas de interferencias

- **802.11g** "Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band".-

  - Se ejecuta en tres canales del espectro de los 2,4GHz (al igual que 802.11 b)
  - Presenta la misma velocidad que 802.11a, pero cuenta con compatibilidad con el estándar 802.11 b
  - Más seguro

Dentro del mercado, el estándar que más aceptación ha tenido es el 802.11b, aunque la velocidad de transmisión máxima (11Mbps) es inferior a la del 802.11a(54Mbps).

La razón es que debido a que se trabaja a una banda de mayor frecuencia (5GHz) el alcance es justo la mitad que en el 802.11b que trabaja en la banda de 2,4GHz. El nuevo estándar 802.11g, que aún está en estudio, trata de llegar a velocidades de transmisión similares al 802.11a, pero en la frecuencia de 2,4GHz.

1.9.2. Punto de Acceso

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".[9]

Gráfico 1.8: ACCES POINT.
Fuente: HTTP://ES.WIKIPEDIA.ORG/WIKI/PUNTO_DE_ACCESO

1.9.3. 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.

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

Gráfico 1.15: SWITCH INALÁMBRICO SYMBOL WS2000.
Fuente: HTTP://WWW.ZETES.COM/ELINK/05Q1/SPAIN/WIRELESS-SWITCH.HTM.

1.9.4. Puente inalámbrico

Cuando se tiene varias LAN y se desean interconectar. Este tipo de redes se puede conectar mediante dispositivos llamados **Puentes,** que funcionan en la capa de enlace, que funcionan en la capa de enlace de datos.

Los puentes examinan las direcciones de la capa de enlace de datos para enlutar los datos. Como no tienen que examinar las direcciones de la capa útil de las tramas que enlutan, pueden transportar paquetes IPv4, IPv6 Apple Talk, ATM, OSI o de otros tipos. En contraste, los enrutadores examinan las direcciones de los paquetes y realizan su trabajo de enrutamiento con base en ellas. Aunque está parece una clara división entre puentes y los enrutadores, algunos desarrollos modernos como el surgimiento de la Ethernet conmutada, han enturbiado las aguas.[10]

1.9.5. Puente multi-punto

Un uso común de los puntos es conectar dos o más LAN distantes, Por ejemplo una empresa podría contar con plantas en varias ciudades, cada una con su propia LAN. En un plano ideal todas las LAN deberían estar interconectadas de tal forma que funcionan como una sola LAN grande.

1.9.6. Antenas direccionales

[10] REDES DE COMPUTADORES, TANENBAUM, Andrew, Cuarta Edición.
Tomado de la Página 318.

Estas antenas son capaces de enfocar toda la señal que le aplica la tarjeta o punto de acceso, a una dirección concreta en función del modelo y características.

Normalmente estas antenas se usan para establecer enlaces punto a punto (direccional con direccional) o para enlazar con un nodo que tenga una antena Omni direccional.

Dentro de la gama de antenas direccionales, existen también varios modelos y formas, cada una con un uso concreto:

1.9.6.1. Antena Direccional de rejilla, o parabólica.

Esta antena está diseñada para establecer enlaces punto a punto o para conectar a un nodo. Se caracterizan por su alta ganancia, que va desde unos 15dBi hasta los 24dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce en gran medida el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8° de apertura.

1.9.6.2. Antena Direccional tipo Patch Panel.

Con estas antenas se consigue crear pequeñas zonas de cobertura, tanto como recintos, estaciones de metro y similares, consiguiendo con varias de ellas establecer 'células' como en telefonía móvil.

Otra utilidad puede darse para sustituir una antena omnidireccional, tras la cual pudiera encontrarse un edificio u otra estructura que impidiera que la señal se propagase, poniendo varias de ellas para

cubrir la zona deseada y no desperdiciar señal. A esta unión de antenas se las llama 'Array'.
Normalmente la anchura del haz que irradian estas antenas es de 25° tanto en vertical como en horizontal.

1.9.6.3. Antenas Omni-Direccionales.

Como su nombre indica, estas antenas son capaces de emitir señal en todas las direcciones, pero esto tiene un pequeño matiz.

La radiación en todas las direcciones, pero esto no es lo que realmente sucede, pues las antenas no emiten señal en todas las direcciones, sino más bien sobre su propio plano pues es aquí en donde se conseguirá la máxima potencia.

Una cosa que pasa de forma bastante habitual, es que se pone la antena en un lugar muy alto, y luego a la altura de la calle no llega la señal pues la antena es omnidireccional sólo sobre su mismo plano.

Con la ganancia de las antenas omnidireccionales pasa algo muy similar a lo que ocurría con las direccionales: cuanto más alta es su ganancia, más estrecha es ia radiación horizontal que estas emiten.

1.10. INSTALACIÓN Y CONFIGURACIÓN DE LAS TARJETAS DE RED

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.

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 (Portátiles)	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**	Sicodélica
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

Tabla 1.1: TABLA DE TARJETAS INALÁMBRICAS (ACTUALIZADO A (3-10-06)
Fuente: HTTP://WWW.SYMBOL.COM.MX/INFO8.HTML

1.11. INTERCONEXIÓN WLAN

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 cualquier lugar 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.

1.12. VENTAJAS Y DESVENTAJAS

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se

encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.

- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

1.13. INTRODUCCIÓN A LA SEGURIDAD

1.13.1. Seguridad en Wlan

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología WLAN 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 WLAN 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 **WLAN** en este momento.

1.13.1. Dispositivos para WLAN

"Existen varios dispositivos que permiten interconectar elementos WLAN, de forma que puedan interactuar entre sí. Entre ellos destacan routers, puntos de acceso, para la emisión de la señal WLAN 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 WLAN 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".[11]

1.14. AMENAZAS

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

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

[11] http://es.wikipedia.org/wiki/Wi-Fi, Tecnologia Wireless Fidelity.

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

1.14.3. 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.

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

1.14.5. 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.

1.14.6. 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 o aplicaciones.

1.14.7. Injection: El atacante puede insertar paquetes en la red inalámbrica causando que todos los clientes se desconecten o inundar la red con paquetes basura (generando un DoS).

1.14.8. Replay: El atacante captura paquetes y luego los reinserta en la red inalámbrica con o sin modificación.

1.14.9. 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.

1.15. MÉTODOS PARA IMPLEMENTAR SEGURIDAD DE UNA RED INALÁMBRICA

1.15.1. 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.

1.15.1.1. Encriptación 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.

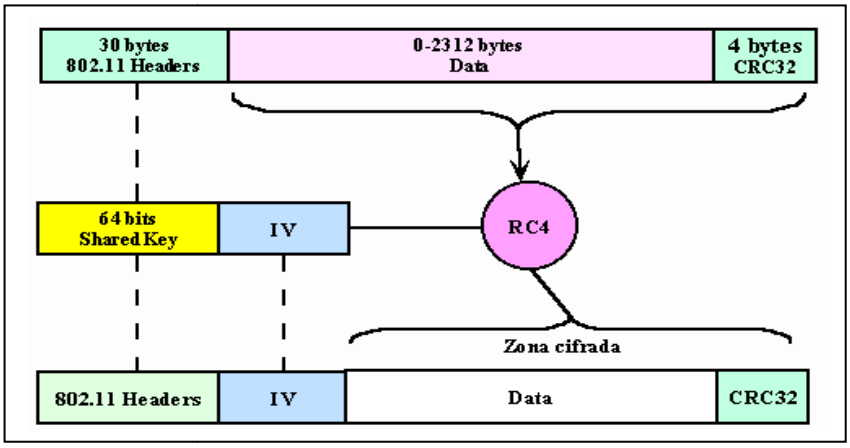


Gráfico 1.16: ALGORITMO DE ENCRIPTACION WEP
Fuente: HTTP://WWW.MONOGRAFIAS.COM/TRABAJOS18/PROTOCOLO-WEP/PROTOCOLO-WEP.

1.16. 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."

De acuerdo a lo expuesto por el autor se considera que, **REDES INALAMBRICAS** es un conjunto de ordenadores que mantiene una estricta relación entre sí 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 inalámbrica para el beneficio de la Fiscalía.

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.

En consecuencia las seguridades en las redes inalámbricas han dejado de ser una utopía, ya que con el avance tecnológico y el aparecimiento de nuevas herramientas y dispositivos inalámbricos con estándares internacionales.

CAPITULO II

2. TRABAJO DE CAMPO

2.1. ELEMENTOS NECESARIOS PARALA CONFIGURACION Y FUNCIONAMIENTO DE LOS ACCESS POINT

Hasta ahora sabemos dos cosas: nos gusta la tecnología Wi-Fi y sabemos que hay una norma (la 802.11) que la regula ¿Pero cómo funciona? Primero entendamos cómo funciona la tecnología inalámbrica. La norma 802.11 está 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) está controlada por una base o 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 ACCESSO POINT

“Normalmente se pueden utilizar Access Point como repetidores de señal o 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”.
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 o 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.

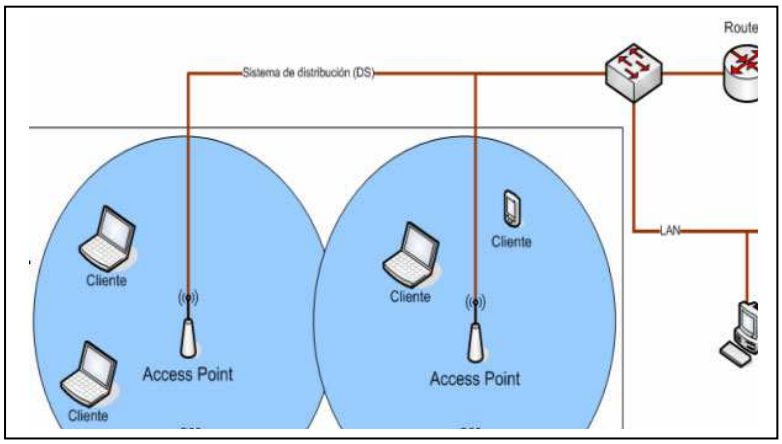
Como se conecta un cliente a una red inalámbrica cuando una PC o

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: LA INVESTIGADORA



2.1.2. METODOLOGIA PARA LA IMPLEMENTACION DE ACCESS POINT (PUNTOS DE ACCESSO)

Para la implementación de puntos de acceso como parte de una metodología debemos tener en cuenta la planificación interior:

Planificación de interior

Como hemos indicado con anterioridad, las simulaciones en OPNET consideran el modelo de propagación en espacio libre y no permiten el modelado de obstáculos. Por ello la fase de planificación de interior se pospone a la fase de realización de pruebas de campo. En el siguiente apartado definiremos la metodología a emplear y las herramientas a emplear en la fase de validación en campo.

Validación en campo

- Ubicación exacta de los APs.
- Tipo de antena y potencia de radiación de cada AP.
- Asignación final de canales.
- Configuración de los controladores de AP para que se encarguen del traspaso de llamadas o handover.
- Configuración del sistema para especificaciones de calidad de servicio.

Estado del arte en la caracterización del canal radio

La caracterización del canal radio es un tema complejo que requiere, por un lado, el conocimiento profundo de señales radioeléctricas, y por otro, el conocimiento sobre la modulación empleada en cada capa física: 802.11b, 802.11g y 802.11n. Además, las prestaciones del canal de radio como interferencias, pérdidas, etc., serán claves en las prestaciones finalmente obtenidas por las aplicaciones. Sin embargo, las capas superiores a la capa física (p.e. la subcapa MAC, normas como 802.11e o incluso el protocolo de transporte) también afectan directamente a las prestaciones obtenidas por las aplicaciones, Por ello, para comprender mejor cómo afecta el radio enlace a las prestaciones recibidas por las aplicaciones es necesario tener una visión de conjunto de todo el sistema WiFi. Esta visión de conjunto se ofrece en una panorámica sobre 802.11 y aclara conceptos básicos como interferencia y fiabilidad asociados a las redes WiFi. También realiza una brillante descripción de los estándares

IEEE 802.11 a través de la capa física (canal radio: modulaciones, frecuencia, etc.) y subcapa MAC (formato de trama, acceso al medio compartido, etc.) de dicha norma. El artículo continúa describiendo los modos de funcionamiento de infraestructura y ad-hoc y los valores típicos de los parámetros más importantes usados en la norma. En dichos valores ya vemos una primera justificación del elevado tiempo de acceso al canal, lo cual podrá afectar a las aplicaciones de tiempo real e interactivo (como voz o videoconferencia). Posteriormente el artículo termina simulando el umbral máximo alcanzable en función de la tasa de error en el canal los umbrales de la norma, dando como resultado un caudal eficaz de entre el 50% y 80% del régimen binario del enlace radio. Finalmente el artículo simula la distribución acumulada del retardo máximo de acceso para el servicio de VoIP obteniendo un acceso menor de 300 ms con una probabilidad de más del 90%.

Sin embargo, nuestro proyecto se encuadra en un entorno industrial. Aunque inicialmente se planea tener un uso “no industrial” de la red WiFi (comunicaciones y una aplicación de almacenes), sería interesante conocer qué requisitos debería cumplir para poder ser empleada en comunicaciones de control industrial. Ello se ofrece en donde se presenta una excelente panorámica sobre la tecnología inalámbrica en entornos Industriales. No sólo se limita a la tecnología 802.11 sino también a redes profibus inalámbricas. El artículo constituye una fuente básica de consulta para el diseño de la red WiFi en nuestro escenario, ya que explica los aspectos claves de las comunicaciones inalámbricas y su influencia en redes industriales. En su sección segunda se explican los problemas fundamentales del transporte de datos en tiempo real dentro de las redes industriales. En particular, se comentan los fundamentos de las propiedades básicas de los enlaces inalámbricos: pérdida en el camino (donde se ofrece una expresión analítica para entornos industriales), operación semi-duplex, cabeceras a nivel físico, errores en el canal y, finalmente, la interferencia entre símbolos. A continuación se describen Problemas típicos en redes inalámbricas en función de la tecnología (consistencia, terminal escondido, etc.) así como sus soluciones. Tras una

breve revisión de las tecnologías inalámbricas en el entorno industrial (Bluetooth, 802.11a/b/g, etc.) se describe la conexión de dichas tecnologías con los entornos cableados y los conmutadores. Como principal aportación del artículo podemos seleccionar el modelo de propagación para entono industrial, así como sus casi 150 referencias bibliográficas.

En lo relativo a la caracterización del canal radio, se puede encontrar un estudio exhaustivo sobre la caracterización del canal radio en entornos industriales cuando utilizamos una modulación OFDM (usada en 802.11a y 802.11n). . El trabajo de investigación revisa a fondo los detalles de la estimación del canal en canales estáticos y con variación en el tiempo. Los estimadores utilizados son los de mínimos cuadrados y el estimador de raíz media lineal. El artículo presenta medidas en entornos industriales para Hiperlan/2. En los resultados se presentan figuras de la probabilidad de pérdida de paquete en función de la relación señal a ruido y el retardo de propagación. Tanto parte de los resultados como la metodología pueden ser reutilizados para la estimación precisa del canal en redes WiFi.

Sin embargo, en nuestro proyecto estaremos más interesados en la medición de prestaciones que se obtienen sobre un determinado canal de radio, que en la caracterización del propio canal radio. Para ello es necesaria una metodología de medición de prestaciones que ofrezca como resultados el retardo y la probabilidad de pérdidas en entornos industriales. Se presenta una metodología para la medición de prestaciones en el canal radio con pruebas y medidas en entornos industriales de características similares a nuestro escenario. Aunque las medidas están hechas para la 802.11, la metodología puede ser igualmente válida en entornos de 802.11b/g/n. El experimento realizado consiste en el envío de sondas (probe) periódicas a distancias de 55 m en una nave industrial. El software utilizado para la generación de tráfico y el análisis de medidas puede ser usado en nuestro proyecto y está disponible para cualquier sistema operativo. En el análisis de los

resultados destaca una probabilidad de pérdida de paquete (PER) de 1e-03 para distancias de 55m y entornos ruidosos. La probabilidad de pérdida se incrementa a medida que se envían paquetes de prueba a una tasa cercana al máximo. Esta metodología puede ser adaptada y mejorada (p.e. en la medición del retardo) para realizar mediciones en nuestro proyecto.

También es conveniente notar que la tecnología de la norma 802.11n permite el uso de múltiples antenas (MIMO) y por lo tanto, múltiples canales radio simultáneamente.

Se analizan y cuantifican las ventajas de usar la redundancia como técnica para incrementar la fiabilidad en entornos inalámbricos industriales. En particular analiza el uso de técnicas FEC y de la redundancia de antenas o MIMO. Esto último nos es de gran utilidad en el proyecto ya que pensamos utilizar dicha tecnología. Tras un análisis preliminar, se valida un modelo analítico que predice la bondad del uso de múltiples antenas frente a la probabilidad de error de paquete de un canal.

Finalmente, conviene disponer de estudios donde no se estudie directamente el canal radio sino los límites de las aplicaciones multimedia que usan un canal radio WiFi (802.11b/g). A este respecto se presentan las características principales del envío de VoIP sobre redes WiFi de forma que se puedan calcular los consumos reales de ancho de banda de una conversación. Como principal resultado tenemos un modelo analítico que analiza el número máximo de conversaciones que simultáneamente pueden tener lugar en un entono de VoIP-WiFi industrial. A este respecto, los resultados obtenidos con el codec G.729 son de 55 conversaciones máximos por punto de acceso con 802.11g (hasta 54 Mb/s) y 11 con 802.11b (hasta 11 Mb/s) en un canal ideal. En el caso de envío de vídeo simultáneo, el número de conversaciones simultáneas se reduce a entre 31 y 3 para 802.11g dependiendo del caudal ocupado por el vídeo (entre 1 y 3Mb/s). Estos son los límites que

podemos esperar en canales ideales. Estos límites se verán reducidos en aquellos puntos de acceso que se encuentren situados en zonas de alto ruido de la fábrica. Sería necesaria una medición usando la metodología indicada para determinar con mayor precisión las prestaciones reales recibidas en dichas zonas.

Finalmente se completa el estudio realizado en sentido de buscar un límite sobre la capacidad de simultanear llamadas de VoIP de los enlaces WiFi. En este caso no se ofrecen análisis analíticos sino simulaciones con OPNET sobre las prestaciones recibidas por N usuarios de VoIP en una red 802.11g. El codec utilizado en esta ocasión es el G.711 (64kb/s). Sus resultados ofrecen un caudal eficaz (throughput) de entre 3 y 7 Mb/s en función de los valores de Backoff configurado en el protocolo de acceso al medio compartido. Ello equivale a la admisión de entre 22 y 48 llamadas simultáneas con una calidad aceptable, obteniéndose un retardo medio en el acceso al punto de acceso de 20ms.

a) La caracterización del canal radio es compleja y para los propósitos del proyecto lo interesante es la caracterización de las prestaciones que las aplicaciones reciben a través de un canal radio de entorno industrial.
b) Para medir las prestaciones de dicho canal radio se propone el seguimiento de una metodología similar a la empleada en donde se mejore el software para medir el tiempo extremo a extremo.
c) El uso de varias antenas (redundancia en canales radio) mejora claramente las prestaciones obtenidas por las aplicaciones. La norma 802.11n permite esta prestación (MIMO). En la actualidad se encuentra normalizado el hardware necesario para implementar dicha norma por lo que es posible encontrar productos comerciales que la implementen. Parece muy interesante el uso de tecnología 802.11n en las zonas de alto ruido industrial donde se requiera la disponibilidad del servicio multimedia.
d) Las prestaciones que podemos esperar de los puntos de acceso en cuanto al número de conversaciones simultáneas de VoIP o envío de voz, datos y vídeo simultáneo, con una calidad media/alta, no presentan

problemas respecto a la demanda esperada en la fábrica. Inicialmente, no existiría problema en que cada punto de acceso manejase un número de conversaciones simultáneas superior a 10. Esto mejora notablemente con el uso de la norma 8011.e o, 8011.n. Por lo tanto, la 802.11n también está recomendada en aquellas zonas donde exista una alta carga de tráfico, aunque no exista ruido industrial.

METODOLOGIA

A la hora de planificar las pruebas de campo hay que segmentar el escenario en varias zonas para facilitar su estudio. Se realizarán mediciones de dos tipos: señal/ ruido y rendimiento con aplicaciones reales. Para que resulte más cómoda e intuitiva la representación de las mediciones nos valdremos de planos de las ubicaciones donde situaremos los APs y los terminales a estudio.

En una fase de pruebas de estas características hay un amplio abanico de experimentos a realizar por lo que tomaremos la simplificación de emplear solo dos terminales y que uno de ellos esté en la ubicación del AP que le da servicio. El terminal situado en el AP estará conectado al mismo vía Ethernet y el otro terminal vía interfaz inalámbrica con un adaptador que implemente el borrador 802.11n.

Las medidas de SNR en el terminal móvil se harán con el software NetStumbler y sus resultados se emplearán para elaborar un mapa de cobertura del terreno. Por otro lado cursaremos aplicaciones entre los dos terminales con el empleo de la herramienta D-ITG que permite emular flujos de tráfico de datos. A continuación describiremos algunas funcionalidades de esta aplicación:

- Posibilidad de emular flujos predefinidos como VoIP (con varios códecs), tráfico TELNET, DNS o posibilidad de definir una fuente de tráfico personalizada (UDP, TCP, ICMP, SCTP).

- Envío de múltiples flujos de distintas especificaciones dirigidos a un mismo receptor.
- Obtención de estadísticas como la pérdida de paquetes, la tasa media Recibida, jitter, retardo medio, etc.

Este software se ejecutará en los dos terminales, uno de ellos actuará como emisor de los flujos y el otro actuará como receptor de las fuentes de tráfico.

Contrastando los resultados en la recepción con lo enviado por el emisor, podremos interpretar el correcto funcionamiento de las aplicaciones. A continuación presentaremos de forma detallada los pasos a seguir a la hora de realizar estas pruebas en el escenario objeto de estudio.

Paso 1: Segmentación

En el primero de los pasos a seguir debemos extraer el plano de la zona segmentada objeto de estudio del plano general de la planta de la fábrica. Resulta interesante que el plano extraído contemple las zonas colindantes que puedan ser afectadas por la radiación de los puntos de acceso instalados en el lugar.

Pasó 2: Inspección de ubicaciones candidatas

Inspeccionar el escenario objeto de estudio y definir varias ubicaciones candidatas a albergar los APs. Las ubicaciones de los APs responderán a los resultados anteriores de las herramientas empleadas en las fases I y II y a las ubicaciones que por sentido común y posibilidad de instalación resulten adecuadas. El terminal móvil bajo prueba se desplazará por ubicaciones alejadas del AP, cercanas a interferencias, “escondidas” por obstáculos, y en definitiva, emplazamientos que hagan al sistema encontrarse en casos más desfavorables de funcionamiento (es indudable que estos lugares quedan a merced del sentido común y la experiencia del instalador).

Las ubicaciones anteriores serán marcadas en el plano con un código de colores que identifique el AP y los terminales en juego. Cada vez que algún elemento sufra un cambio en su posición, ya sea un AP o un terminal, estaremos definiendo un nuevo escenario. El concepto de escenario nos permite definir una nomenclatura que incluya la zona objeto de estudio, la posición de los elementos y el perfil aplicado para así ordenar los datos que vayamos obteniendo a raíz de las pruebas. Por ejemplo, los datos con el siguiente etiquetado: ZI1E0M02, corresponden a la zona interior 1, el escenario 2 y la aplicación del perfil de medida 2.

Pasó 3: Medidas canal radio

Con el terminal móvil objeto de estudio tomaremos una serie de mediciones antes de aplicar ningún tipo de tráfico. Estas serían las siguientes:

- Velocidad interfaz (Mbps). Valor obtenido en la aplicación de la tarjeta del portátil receptor. Hemos tomado la velocidad de la interfaz en transmisión.
- Señal recibida (dBm). Obtenida por la aplicación de la tarjeta del portátil receptor.
- Ruido (dBm). Obtenido por la aplicación de la tarjeta del portátil receptor.

Como podemos apreciar son las mediciones asociadas al canal radio propiamente dicho y dan una idea cualitativa del comportamiento que tendrá el terminal al aplicarle tráfico real.

Pasó 4: Inyección de tráfico real

Inyección del perfil de tráfico de la zona objeto de estudio mediante el software D-ITG, el extremo emisor será el terminal móvil y el extremo receptor será el ubicado en el emplazamiento del AP. La nomenclatura empleada en los perfiles es la siguiente:

VoIP/Telnet/Video/Servicios

Por ejemplo, un perfil 15/10/4/3 incluiría 15 fuentes de voz IP, 10 fuentes Telnet, 4 fuentes de video streaming y 3 fuentes de servicios generales (consulta a Webs, correo, etc.). De esta forma nos resulta cómodo identificar los distintos perfiles empleados en las distintas zonas.

Los perfiles aplicados a cada AP individualmente son el total de las aplicaciones para toda la zona a estudio, de esta manera estamos sobredimensionando, ya que aplicamos todos los usuarios previstos en la zona a un único punto de acceso. En la realidad estos perfiles y número de usuarios estarán repartidos entre los puntos de acceso ubicados dentro de la zona de estudio, por lo que la carga queda repartida entre varios equipos. En todos los escenarios aplicaremos esta prueba de tráfico real, para averiguar si el sistema soporta este pico de utilización del canal radio. Esta medida tiene el identificador M01.

La segunda prueba a aplicar en cada uno de los escenarios viene destinada a ver el ancho de banda máximo alcanzable en cada ubicación.

Este ancho de banda máximo está determinado por la distancia desde el emplazamiento hasta el punto de acceso, esta distancia y el número de obstáculos e interferencias es la que determina la SNR recibida y por tanto el ancho de banda máximo que se puede alcanzar. Este perfil genérico para alcanzar el ancho de banda máximo es el que obtiene el máximo caudal del borrador 802.11n en la configuración de canalización de 20 MHz del punto de acceso (experimentalmente hemos obtenido unos 96 Mbps en el nivel de aplicación).
Esta medida tiene el identificador de M02.

Pasó 5: Análisis de resultados

Si no se ha interrumpido la comunicación vía radio, los paquetes serán recibidos en el extremo receptor y se generará en él un log que se analizará para obtener de él los siguientes datos:

- Pérdidas de paquetes (%). Obtenidas por la aplicación D-ITG empleada para generar el tráfico real.
- Jitter (ms). Obtenido por la aplicación D-ITG empleada para generar el tráfico real.
- Retardo medio (ms). Obtenido por la aplicación D-ITG empleada para generar el tráfico real.
- Ancho de banda recibido (Mbps). Obtenido por la aplicación D-ITG empleada para generar el tráfico real.

Los resultados aparecen como totales de las medias de los flujos implicados y también individualmente por cada fuente de tráfico.

Pasó 6: Solución

El análisis de resultados nos permite obtener una solución que debe ser sustentada en las siguientes premisas:

- Cobertura global de la zona.
- Mínimo número de puntos de acceso en la zona.
- Requisitos de las aplicaciones cumplidos, en cuanto a retardo, jitter y pérdida de paquetes se refiere.
- Viabilidad de instalación en las ubicaciones escogidas.

La solución quedará reflejada en un escueto informe por cada una de las zonas segmentadas del plano total del escenario completo. En el siguiente apartado presentamos un ejemplo para ilustrar al lector.

2.2. ENTREVISTAS A LOS TECNICOS DE LA DIRECCION DE SERVICIOS INFORMATICOS DE LA UNIVERSIDAD TECNICA DE COTOPAXI COMO APOYO TECNICO EN LA ELABORACION DEL PRESENTE TRABAJO DE INVESTIGACION.

2.2.1. Entrevista al Director de Servicios Informáticos de la Universidad Técnica de Cotopaxi.

Como parte del desarrollo de la tesis se realizó una entrevista al Ing. Adrián Mena Rojas Director de la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi por la experiencia adquirida a lo largo de todos los años que ha venido laborando en los laboratorios de sistemas y luego en los laboratorios del CEYPSA.

Para la Entrevista se planteó como principal objetivo conocer cuáles son las expectativas que se crean en las autoridades, personal administrativo y docentes de la Universidad Técnica de Cotopaxi el realizar alternativas de equipos concentradores de información ya que esto hace que se pueda optimizar los recursos con que cuenta la Universidad.

El Director de Servicios Informáticos considera que es importante cooperar con el avance tecnológico y más aún si va en beneficio de esta importante dependencia, que se encarga de impartir conocimiento a la juventud de la ciudad de Latacunga y de la provincia de Cotopaxi.

Afirma que a nivel nacional temas de investigación de este tipo son de gran beneficio para los profesionales del área de informática y sistemas, por lo que siempre se ha hecho urgente el tratar de capacitar al personal técnico de sistemas. Pero también nos manifestó que la Universidad al ser una de las más nuevas no tiene el presupuesto suficiente para poder capacitar a su personal dentro de las aéreas que se consideran criticas

esto hace que la dirección tenga que mirar a otros lados como a los proyectos de investigación que generan las carreras de la Universidad y muy particularmente a las de Ingeniería en Informática y Sistemas Computacionales.

Al momento en la bibliotecas se pudo observar que constan muchos trabajos de investigación orientados a las redes de comunicaciones de datos y a las implementaciones de redes inalámbricas tanto en la matriz de la Universidad como en el campo del CEYPSA y en la sede de la Mana, pero en ninguno de estos casos se pudo desarrollar una investigación de un concentrador mediante una computadora que es lo que se está planificando de parte de la persona investigadora, el cual mediante la utilización de software libre se lo podrá realizar sin costo alguno al menos en lo que tiene que ver con el pago de licenciamiento.

2.2.2. Entrevista al Director del presente tema de Investigación.

Todo trabajo de investigación que vaya en beneficio de la Universidad siempre será un aporte y más cuando se trata de optimizar los recursos tecnológicos, contando siempre con que la institución en la que laboramos y estudiamos como es su caso siendo público está en la obligación de realizar una migración urgente entre plataformas tecnológicas como lo es de software propietario como Windows 2003, aplicativos de Microsoft Visual Studio C#. Net, SQL Server 2005, hacia lo que es Linux como sistema operativo, las aplicaciones a Open Source sea este Java o php y como motor de Bases de datos al MySql.

Un Access Point mediante un computador personal sería de gran aporte no solamente para la universidad sino para la comunidad en general ya que es un aporte tecnológico para todos aquellos que tienen conexiones a internet y que cuentan con una tarjeta de red inalámbrica.

El sistema operativo Linux es una herramienta muy poderosa que hay que saber explotar ya que ofrece muchas bondades tecnológicas, y lo

mejor es que muchas de las versiones se encuentran en el internet de forma gratuita y solamente hay que descargarles, por otro lado investigar para poder realizar un concentrador siempre es beneficio para la Universidad y para ustedes como estudiantes ya que de esta manera se trata de que aprovechen los recursos con los que ustedes cuentan no se hacen grandes inversiones como el implementar antenas que son costosas y que a la larga para un domicilio jamás va a justificar por el costo más que todo, en Linux al contar con un firewall administrable

2.2.3. Análisis de la entrevista al Ing. Adrián Mena Rojas, Director de Servicios Informáticos de la Universidad Técnica de Cotopaxi

La universidad en la actualidad cuenta con la mejor tecnología que se puede encontrar en el mercado y los procesos se cambian para mejorar existen aplicaciones con son de óptima calidad el hardware que se ha adquirido a mejorado el rendimiento, pero a nivel de investigación considero que hay mucho que hacer ya que existen investigaciones de muchos estudiantes que se han quedado en la biblioteca como letra muerta.

Al proponer el tema de investigación al personal de esta dependencia le parece interesante pero que no puede ser implementado a nivel de departamento de sistemas ya que el hardware de redes es mucho más importante ya que tiene una mayor cobertura es, es más estable obviamente que no se pudiera equiparar un servidor doméstico como el de la investigación con la tecnología que puede tener un Access point o router inalámbrico que son dispositivos que se han hecho para cubrir una vasta área de cobertura y de réplicas para otros equipos que disponen de alguna tarjeta inalámbrica para poder acceder a un equipo o servicio de red inalámbrica.

Para la investigación fue un aporte valioso el poder contar con el aporte de los profesionales que cuenta la Universidad ya que el criterio técnico de esta gente siempre es un aporte positivo para cualquier investigación y

más cuando se genera alternativas de la tecnología que existe en la actualidad.

2.2.4. Análisis de la entrevista del Director del tema de investigación

La contra posición resulto la entrevista a un docente de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas ya que resulta que este tipo de temas engrandece aún más el prestigio de la universidad toda vez que se esté brindando alternativas válidas de tecnología al poner en consideración una alternativa válida de compartir recursos e información.

Conversar con los docentes sobre algunos avances tecnologías siempre es positivo para todo trabajo de investigación y más aún cuando se trata de redes y comunicaciones por cuanto este campo se encuentre en permanente cambio tecnológico, sin descuidar claro el aspecto de software que cubre un amplio campo dentro del área de la Informática y los sistemas computacionales.

Todas las entrevistas estuvieron llenas de valiosos aportes y se ha creído conveniente tomar en cuenta estas dos por tratarse de lo más representativo por lo mencionado.

2.2.5. Comprobación de la Hipótesis.

En el plan de tesis se planteó como hipótesis:

Con la construcción de un Punto de Acceso (AP) mediante una computadora personal utilizando GNU/Linux para administrar recursos como servidor de archivos, internet y firewall se puede optimizar recursos tanto de tiempo como económicos.

La presente investigación tuvo como objetivo fundamental el brindar algunas alternativas para compartir recursos tecnológicos como el internet, y sobre todo el tratar de que equipos que en algunos casos son considerados como obsoletos puedan entrar en funcionamiento para que sirvan de servidores de otros equipos que no cuentan con dos o más tarjetas de red.

De igual manera se plantea en herramientas de tipo Open Source (Código Abierto), como es el sistema operativo Linux CentOS en su versión 5 ya que en la actualidad es el sistema operativo de este tipo más robusto del mercado,

Al tratarse de esta Nobel tecnología todos queremos adentrarnos pero pocos lo han conseguido con éxito, esto con respecto a la resistencia que se encuentra de parte de los empleados a querer adaptarse a nuevos procesos y a las capacitaciones que en ocasiones han causado malestar.

CAPITULO III

3. PROPUESTA DE LA CONSTRUCCION DE UN PUNTO DE ACCESO MEDIANTE UNA COMPUTADORA PERSONAL UTILIZANDO LINUX.

3.1. Tema

Construcción de un Punto de Acceso (AP) mediante una computadora personal utilizando GNU/Linux para administrar recursos como servidor de archivos, internet y firewall

3.2. Presentación

Día con día hemos venido observando el vertiginoso avance tecnológico a nivel mundial tanto en el área de informática como en otras áreas, uno de los recursos más importantes dentro del área de informática son las redes de comunicaciones y uno de los objetivos primordiales es la explotación total del procesamiento y la distribución ordenada de los recursos más valiosos como es la información, permitiendo obtener mejoras significativas para el buen desempeño de las instituciones tanto públicas como privadas; ya que gracias a este análisis se han logrado optimizar recursos humanos y financieros, de esta manera obteniendo un adecuado manejo y control de la información.

Debido al rápido progreso de la tecnología, estas áreas están convergiendo rápidamente y las diferencias entre juntar, transportar, almacenar y procesar información desaparecen con rapidez. Las organizaciones que se extienden sobre una amplia área geográfica esperan ser capaces de examinar la situación o administrar sus recursos, aún de sus más remotos puestos de avanzada, oprimiendo un botón, de esta manera crece nuestra habilidad para obtener, procesar y distribuir información, también crece la demanda de técnicas de procesamiento de información avanzada.

En cuanto al desarrollo tecnológico del país éste recurso se ha visto diezmado ya que el crecimiento tecnológicamente ha sido incipiente, sin embargo con la tecnología con la que cuenta no ha permitido realizar aplicaciones de tecnologías de red que sean de gran utilidad para el buen desenvolvimiento de las instituciones que se encuentran en nuestro alrededor y así como empresas en particular.

En cuanto al ámbito local, en la que podemos mencionar algunas empresas industriales, plantaciones de flores, a nivel de educación mencionar algunas instituciones de educación superior cuyo objetivo primordial es la de involucrarse en tecnología, este es el caso de la Universidad Técnica de Cotopaxi, todas estas empresas e instituciones estamos conscientes necesitan optimizar sus recursos tanto de software como de hardware, por este motivo creemos oportuno plantear el desarrollo de un Access point o punto de acceso inalámbrico cuya principal herramienta va a ser un computador personal lo cual que puede ser considerada una utopía, pero que puede ayudar de gran manera ya que con el desarrollo de esta investigación se puede optimizar equipos informáticos y que a su vez puede ser de gran utilidad en el aspecto pedagógico de los futuros profesionales de informática de nuestra Universidad.

A lo expuesto anteriormente y ante la necesidad existente de mejorar la funcionalidad de los servidores que tienen todas las empresas e instituciones y que académicamente se potencie el plan académico de los estudiantes hemos propuesto “Construcción de un Punto de Acceso(AP) mediante una computadora personal utilizando GNU/Linux para sus distintos servicios” el mismo que será de gran utilidad para el buen desempeño y la buena administración de la información mediante la utilización de estas herramientas de última generación que ayudarían de buena manera tanto a los administradores de redes de cualquier departamento de Sistemas.

3.3. Justificación

La implementación de un Access Point en procesos críticos que tienen muchas instituciones, resulta muy importante al momento de brindar servicios de calidad a

los usuarios de computadores, ya que al optimizar recursos tanto espacio físico como económico va a garantizar la seguridad de la información y evitando de esta manera la alteración o perdida de la misma.

La necesidad e importancia de desarrollar este tema es porque, se propone dar solución a los problemas como detectar conflictos, invasión, daños en la red, cuellos de botella, deficiencia en el servicio de Internet y acceso a los recursos compartidos, debido a que ésta por ser de carácter tecnológico debe estar en constante actualización; y la falta de un plan estratégico ocasionara el incumplimiento de los objetivos y metas propuestas por las entidades en donde se plantee la utilización de servidores; además porque cada área debe estar interrelacionada para un mejor desenvolvimiento de toda institución.

Por esta razón considerando importante investigar este tema, he escogido él mismo que va a beneficiar a la Universidad donde estudie para realizar un análisis, diseño y posterior desarrollo de un Access Point en un sistema operativo ahora ya muy difundido como lo es LINUX, sin la utilización de muchos recursos físicos como lo son servidores los cuales tiene un elevado costo y que naturalmente ocupan un espacio que en muchas instituciones se los debe optimizar.

Este análisis se realizara basándose en los conocimientos adquiridos en capacitaciones que se las ha realizado luego de haber terminado el ciclo de estudios universitarios, en la experiencia adquirida en mi lugar de trabajo el mismo que se encuentra en un proceso de actualización y de optimización de sus recursos y de igual manera brindar una alternativa válida para que la Universidad entre en este proceso de actualización y de mejorar el nivel académico de los estudiantes de Ingeniería en Informática y Sistemas Computacionales.

3.4. Objetivos

3.4.1. Objetico General

Construir un Punto de Acceso (AP) mediante una computadora personal utilizando GNU/Linux para administrar recursos como servidor de archivos, internet y firewall.

3.4.2. Objetivo Especifico

- Conocer de manera óptima la utilización de las herramientas que permiten realizar concentradores físicos para el desarrollo y pruebas.

- Realizar un estudio de calidad y servicio en los equipos físicos y detectar posibles fortalezas y falencias en las redes de comunicación.

- Despertar la inquietud de investigación tanto de docentes como estudiantes de la carrera de Ingeniería en Sistemas por conocer nuevas herramientas.

- Probar que un Access Point simulado en una computadora personal tiene el mismo potencial que tiene el equipo físico, si se los utiliza de buena manera

3.5. Análisis

Para poder realizar un análisis completo del desarrollo de un punto de acceso inalámbrico mediante la utilización de una computadora personal debemos tener en cuenta algunos conceptos, metodologías y estándares que va a ser repetidos durante la propuesta del desarrollo de la investigación:

3.5.1. Mecanismo de acceso

Hay de dos tipos:

Protocolos con arbitraje (FDMA - Frequency División Múltiple Access, TDMA - Time División Múltiple Access)

Protocolos de contienda (CDMA/CA - Carrier-Sense, Múltiple Access, Colusión Avoidance), COMA (Code División, Múltiple Access) y el CDMA/CD (detección de colisión).

3.5.1.1. Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).
Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

3.5.1.2. Protocolos de acceso por contienda

Tienen similitudes al de Ethernet cableada de línea normal 802.3:

3.5.1.2.1. CSMA

(Code-division múltiple access = Acceso múltiple por división de tiempo).

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia. En este esquema se asigna una secuencia distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias pertenecientes a los demás nodos.

Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

3.5.1.2.2. CSMA/CD

(Carrier Sense, Múltiple Access, Collusion Detection)

En medios de transmisión tales como radio e infrarrojos, no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseñó una variación denominada detección de colisiones (peine) para redes inalámbricas.

En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria pseudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama.

A continuación, el nodo realiza la detección de la portadora si el canal está ubre transmite la secuencia del peine. Por cada "1" del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada "O" del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

3.5.1.2.3. CSMA/CA

(Carrier-Sense, Múltiple Access, Colusión Avoidance)

Es el más utilizado, este protocolo evita colisiones en lugar de descubrirlas.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones.

En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación

de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI.

Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible.
Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802. 11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido).

3.5.2. Seguridad

En el estándar se dirigen suministros de seguridad como una característica optativa para aquellos afectados por la escucha secreta, es decir, por el "fisgoneo". Incluye dos aspectos básicos: autentificación y privacidad.

La seguridad de los datos se realiza por una compleja técnica de codificación, conocida como WEP (Wired Equivalent Privacy Algorithm).

WEP se basa en proteger los datos transmitidos en el medio RF, usando clave de 64 bits y el algoritmo de encriptación RC4 (desarrollado por RSA Security Inc.). La clave se configura en el punto de acceso y en sus estaciones (clientes wireless), de forma que sólo aquellos dispositivos con una clave válida puedan estar asociados a un determinado punto de acceso.

WEP, cuando se habilita, sólo protege la información del paquete de datos y no protege el encabezamiento de la capa física para que otras estaciones en la red puedan escuchar el control de datos necesario para manejar la red. Sin embargo, las otras estaciones no pueden distinguir las partes de datos del paquete.

Se utiliza la misma clave de autentificación para encriptar y desencriptar los datos, de forma que solo las estaciones autorizadas puedan traducir correctamente los datos.

3.5.3. Funcionalidad adicional

En las LAN inalámbricas la capa de MAC, además de efectuar la función de controlar el acceso al medio, desempeña otras funciones;

Fragmentación
Control de flujo
Manejo de múltiples tasas de transmisión
Gestión de potencia

En los diferentes tipos de LAN por cable es posible usar tramas grandes gracias a errores de bit bajos. En las LAN inalámbricas, el multicamino y

las interferencias pueden elevar considerablemente los valores de errores de bit.
Para poder transmitir eficientemente por estos medios, hay que reducir el tamaño de las tramas. La capa MAC se encarga de fragmentar las tramas en otras más pequeñas antes de transmitirlas por el medio inalámbrico.

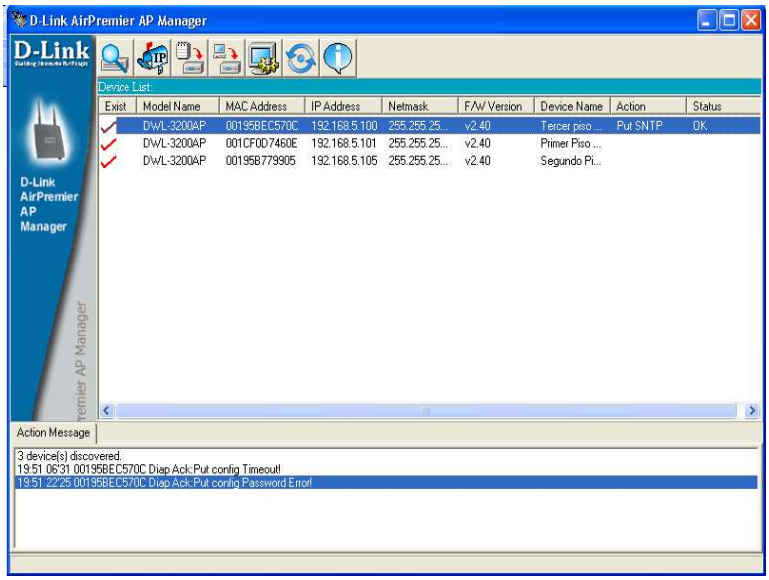
De la misma manera deberá ensamblar las tramas para obtener la trama original antes de entregarla a la capa superior.

También debe cumplir un control de flujo, cada vez que un segmento sea pasado a la capa física, deberá esperar que este sea transmitido antes de enviar el próximo segmento.

La gestión de la potencia se apoya en el nivel MAC para esas aplicaciones que requieren movilidad bajo el funcionamiento de la pila. Se hacen provisiones en el protocolo para que las estaciones portátiles pasen a "modo dormido" durante un intervalo de tiempo definido por la estación base.

Gráfico 3.1: Pantalla de Detección de los AP.

Fuente: La Investigadora



En la parte superior observamos un gráfico de la configuración de los Access Point mediante las direcciones MAC(Funcionalidad), esto con el fin de ver las réplicas que tiene, un dispositivo físico como concentrador y distribuidor de ancho de banda inalámbrico para repartir recursos tecnológicos.

3.5.4. Pasos básicos para asegurar una WLAN

El propósito de asegurar correctamente un punto de acceso(AP) es cortar el paso desde el exterior a nuestra red a personas que no tienen el permiso de entrar, es decir asegurar que la información fluya internamente.

Una red wireless es por definición más difícil de proteger que una red convencional o cableada entre otras cosas porque el medio es el aire y así como en una LAN tenemos una toma de red determinadas y controladas, en principio, en una WLAN se puede acceder desde cualquier punto que permita la antena.

A pesar de esto siempre se pueden establecer una serie de medidas básicas pero efectivas no en el 100% de los casos pero se impide el acceso a la gran mayoría de los intrusos.

3.6. Factibilidad

3.6.1. Factibilidad Técnica

El desarrollo de un proyecto en el cual se va a reforzar un departamento de sistemas, y las seguridades de la información es principalmente influenciado por 3 grandes objetivos los mismos que deben ser cumplidos para poder alcanzar la factibilidad técnica:

- **Resolver un problema:** *Esto es cuando ya existe un servidor implementado ya sea para Proxy o firewall y este tiene procesos que ya no satisfacen el desempeño para lo cual fue creado y es necesario hacerles ciertas modificaciones.*

- **Dar respuesta a directivos:** Cuando se hacen modificaciones de tecnología de la información y las comunicaciones y forzosamente es necesario cambiar el sistema de información o hacerle modificaciones que mejore luego aprovechar esta oportunidad ya que, si de por si se va a hacer un cambio de sistema de información se puede hacer el cambio con las nuevas disposiciones legales y con esto seguir siendo competitivo.

- **Aprovechar una oportunidad:** Un cambio ya sea para ampliar o mejorar el rendimiento económico de la empresa y su competitividad.

Para alcanzar estos objetivos, las empresas emprenden proyectos por una o más de las siguientes razones: capacidad, control, costo, comunicación y competitividad como se lo menciona dentro del Análisis y diseño de Sistemas de Comunicación y Datos.

Capacidad: Las actividades de la empresa están influenciadas por la capacidad de ésta para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas estas son:

- Aumento de la velocidad de procesamiento.
- Permiten el manejo de un volumen creciente de transacciones.
- Recuperan con rapidez la información.

Control: La falta de comunicación es una fuente común de dificultades que afectan a todos los que laboran en una empresa. Sin embargo, los sistemas de comunicación bien desarrollados tratan de ampliar la comunicación y facilitan la integración de funciones individuales.

Aumento de la comunicación: Muchas empresas aumentan sus vías de comunicación por medios de redes.

Costo: Muchas empresas han desaparecido y muchas otras imposibilitadas para alcanzar el éxito debido al poco control sobre los costos o por el total desconocimiento para el control de estos. Los sistemas de información juegan un papel importante tanto con el control como en la reducción de los costos de operación.

Ventaja competitiva: Los sistemas de información y las comunicaciones son un arma estratégica que puede cambiar la forma en cómo compite la empresa en el mercado. Los sistemas de información y las comunicaciones mejoran la organización y ayudan a la empresa a ser más competitiva. Por lo contrario si los competidores de la empresa tienen sistemas de información más avanzados, entonces los sistemas de

información y comunicación pueden convertirse en una desventaja competitiva. Por lo tanto las capacidades de los sistemas de información son una consideración importante al formular la estrategia de la empresa.

Una empresa puede ganar ventaja competitiva a través de su sistema de información y comunicación en cuatro formas diferentes que garantizan la competitividad en el mercado estos son: clientes, competidores, proveedores y servicios.

Todo proyecto de sistemas de comunicación debe ser desarrollado bajo las actividades de un grupo de trabajo que se haga responsable del inicio y culminación del sistema de información.

El grupo de trabajo va a depender de tamaño de acuerdo al proyecto que va a desarrollarse.

Vamos a mencionar los puestos claves de un grupo de trabajo pero podría ser más grande o más pequeño o a veces una sola persona puede desarrollar varios puestos, claro como se dijo anteriormente va a depender de esto el tamaño del proyecto. Por tal motivo solo muestra la apreciación personal de acuerdo a la experiencia profesional que se tiene este tema de investigación

3.6.2. Factibilidad Económica

Al tratarse de seguridades y de compartir recursos como lo es el Internet siempre puede sonar a gastos extremadamente fuertes, pero al tener las empresas e instituciones instalado equipos de última generación y en algunos casos configurables como son los casos de las computadores personales que pueden trabajar como servidores claro con la ayuda de las

nuevas tendencias tecnológicas o en el caso de sistemas operativos como Microsoft crean sus propias configuraciones dentro del propio Windows y cuando tienen estas opciones hay que adquirir paquetes complementarios.

Al contar con todo implementado nuestro trabajo y el de los administradores de los departamentos de Sistemas fue de otorgar una configuración para cada servicio y de esta manera se puede asignar puertos y protocolos que va a servir de enlace entre los servidores y los usuarios de la red, cabe recalcar que siempre es bueno tener más de una tarjeta de red la misma que pueden ser asignadas para cada uno de los recursos.

Lo que se desea llegar es a proporcionar a las empresas una alternativa de Internet a bajos costos utilizando normas y protocolos de Internet, para permitir a los miembros de una organización comunicarse y colaborar entre sí con mayor eficiencia, aumentando la productividad.

La factibilidad económica está dada por la implementación de un corta fuegos (firewall) y un servidor Proxy los mismos que regularían el acceso a la Intranet y el servidor de firewall existente pasaría a controlar tanto interna como externamente.

3.6.3. Factibilidad Operacional

Un servidor Proxy hace de un portero entre la intranet y el Internet o entre ciertos servidores de archivos y la intranet. Cuando una maquina cliente tiene prohibido solicitar directamente a los servidores en nombre de la maquina cliente. Los servidores Proxy pueden también comprobar el tráfico de entrada. Al igual que en un encaminador, un servidor Proxy verifica las reglas que el administrador ha listado (para ver si el contacto

está autorizado) antes de permitir el paso de tráfico. Los servidores Proxy son específicos para las aplicaciones, por ejemplo los servidores Proxy de correo protege al servidor de correo y un servidor Proxy, FTP protege al servidor de FTP.

Los servidores Proxy también pueden inspeccionar el contenido de un paquete y aceptarlo o rechazarlo, según las reglas del administrador. Así, si un servidor Proxy para cualquier servicio contiene una regla de negación, este simplemente niega la acción, así de forma general este diga que se lo debe realizar.

Los servidores Proxy pueden examinar, más cosas que la dirección.

Los intrusos extremos del tipo humano van desde el curioso al maligno y a los individuos motivados por el beneficio económico. En su mayoría, los piratas solían ser estudiosos y experimentados benignos. Los primeros piratas veían el ciberespacio como un lugar público gigantesco de juegos electrónicos y en realidad, más bien como un puzzle absorbente y desafiante. El intento de entrar en un sistema (y salir sin que los atrapasen) era un deporte de competición.

Un intruso puede inyectar un virus o piratear e interceptar, cambiar o robar datos. Y lo hacen. El espionaje industrial es uno de los crímenes informáticos en auge y una vía de ataque.

Todavía hay muchos piratas que pretenden asustar, que se cuelan y miran pero no hacen daño real. Aunque su intrusión es fastidiosa, su principal motivación es la sensación de logro y poder. A su manera, su atención hacia nuestra red puede ser positiva y puede servir para recordarnos que siempre somos vulnerables y para poner de relieve algunas deficiencias especificas en nuestra protección

3.7. Configuraciones

Para la elaboración del presente trabajo de investigación se partió de la implementación de una tarjeta de red inalámbrica en un computador de escritorio o la configuración de la existente en los computadores portátiles, ya que este es un requisito indispensable tener cuando menos dos tarjetas inalámbricas ya que la primera haría de matriz al conectarse con el internet.
Mientras que la segunda tarjeta es decir la tarjeta de red inalámbrica haría de proxy mediante el proxy que se encuentra ejecutado en el Linux Centos, al igual que el firewall que será el que garantice el ingreso y egreso de información hacia y desde los computadores que estén interconectados en la red inalámbrica mediante el computador personal que está haciendo las veces de Access point.

Linux tiene como característica fundamental que las configuraciones se las deben hacer al instalar ya que estas serán las que levanten todos los procesos del concentrador virtual que levantara la maquina personal. Los comandos que se envían a través de consola de Linux son los típicos para realizar un proxy mediante el squid y mediante iptables para lo que es el firewall.

Gráfico 3.2: Configuración DHCP.
Fuente: La Investigadora

Cuando instalamos el servidor de Linux en el computador personal tomamos en cuenta el servidor de dhcp del servidor Linux el mismo que ayudara a que los usuarios del concentrador lógico tomen una dirección IP dinámica que serían a

partir del 192.168.0.100 de ahí en adelante adjudica el servidor de Linux previa configuración del servidor como 192.168.0.1.

Luego de habilitar el dhcp se procede a ingresar a la dirección IP estática para que los usuarios puedan ver a través de esta red todas las conexiones del servidor de redes inalámbricas que simula ser un punto de acceso inalámbrico con las debidas seguridades.

Gráfico 3.3: Configuración Interfaz de red.

Fuente: La Investigadora

En el grafico anterior ya se puede observar las configuraciones de la red inalámbrica la misma que es una clase C en donde se puede observar que hemos tomado en cuenta solamente la versión 4 de IP y mas no la dirección IPv6 ya que esta podría generarnos algunos conflictos al momento de configurar el squid para el proxy o el iptable para el firewall.

El firewall de Linux para el punto de acceso lo configuramos de igual manera con el asistente pero para ciertos servicios ya que le resto de servicios se los realizara mediante comandos propios del centos, como se lo puede observar en el grafico los servicios de comunicación son solo los necesarios y los de páginas web es decir el servidor apache (httpd).

Gráfico 3.4: Asistente de configuración de Firewall

Fuente: La Investigadora

En las configuraciones para el punto de acceso de la red inalámbrica debemos tomar en cuenta las configuraciones de las tarjetas de red inalámbrica dentro de lo que es el sistema operativo Windows XP el m ismo que fue tomado para realizar las practicas necesarias tanto por su versatilidad como por su robustez.

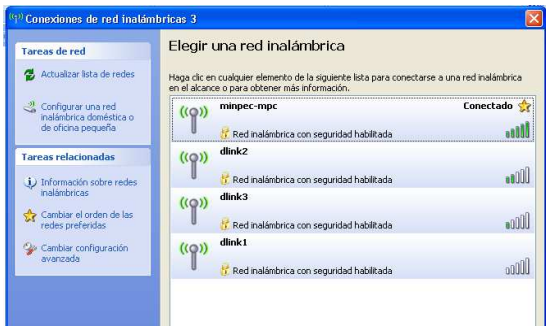
Gráfico 3.5: Configuración tarjeta de Red Inalámbrica.

Fuente: La Investigadora

En la gráfica anterior podemos observar como la tarjeta inalámbrica detecta la cobertura que tiene, que en nuestro caso dispone de 100Mbps para lo que es la red LAN.

Gráfico 3.6: Configuración tarjeta de Red Inalámbrica.

Fuente: La Investigadora

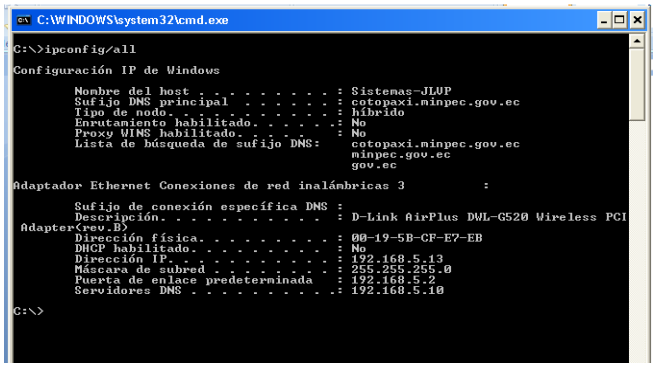


En el sitio donde se nos prestó las facilidades para realizar las prácticas se podían contar con dispositivos fiscos de punto de acceso los mismos que fueron capturados por nuestra red inalámbrica.

De igual manera podemos darnos cuenta que nuestros equipos disponen de un muy buen radio de cobertura el mismo que no está limitado para ningún número de usuarios.

Gráfico 3.6: Configuración Dirección IP de la Red Inalámbrica.

Fuente: La Investigadora



Podemos observar como el DHCP asigna la dirección IP dinámica a la computadora que solicita este servicio.

3.7.1. Diseño Físico de la Red Inalámbrica y Accesos

El diseño físico de la red tiene que ver con la interconexión de computadores y/o componentes digitales (Computadores, PDA, celulares, etc...) que se encuentren cerca del dispositivo que nos hallamos configurando el mismo que utiliza dispositivos de corto alcance los mismos que se encuentran interconectados entre si dentro de un rango no mayor a 10m, para que puede replicar la señal.

Si se desea que el punto de acceso replique su señal, la distribución física de los equipos AP´s se lo deberá realizar de forma que puedan ser vistos unos con otros es decir que permita las réplicas de la señal dentro de todo el edificio.

Es necesario dar a conocer que la señal alcanza incluso el exterior del edificio razón por la cual se ha tomado las seguridades anteriormente expuestas, ya que de esta manera hemos evitado que se puedan dar los ataques de piratas informáticos (hackers).

3.7.1.1. Medidor de señales de la red inalámbrica

Para medir el alcance de la señal se procedió a descargar un rastreador de señales de redes inalámbricas el cual detecta AP’s o computadores que se encuentren en el alcance, como se puede observar en la gráfica que se encuentra más adelante en donde se puede observar al XIRRUS buscando dispositivos dentro del alcance.

Gráfico 3.7: rastreo en forma de radar
Fuente: La Investigadora

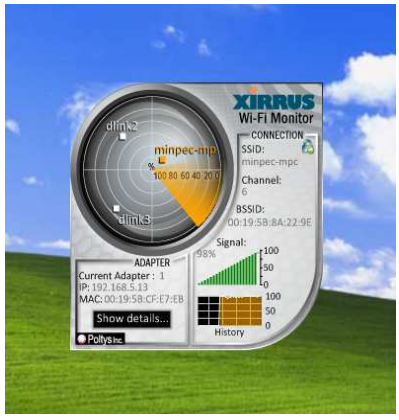
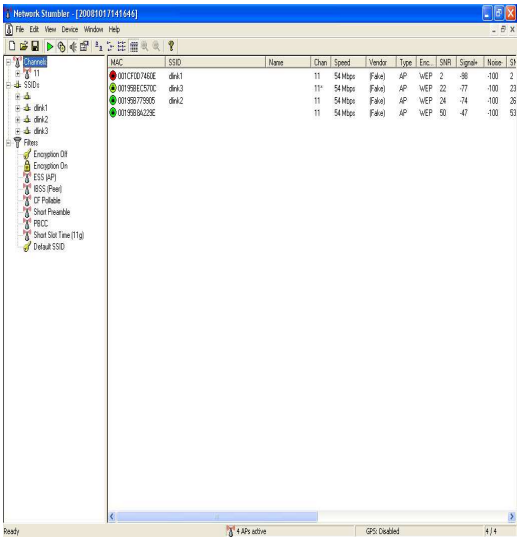
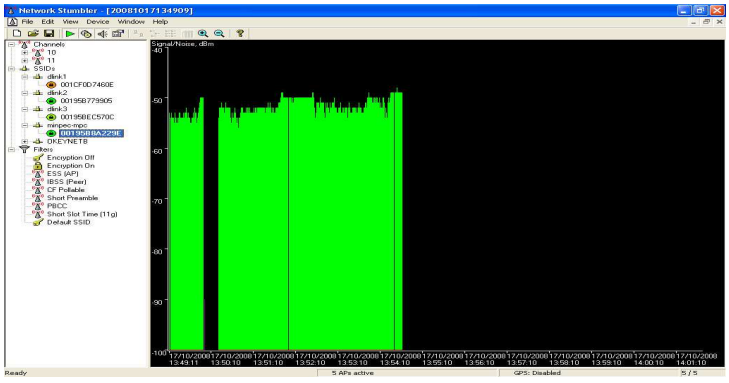


Gráfico 3.8: rastreo en forma de radar
Fuente: La Investigadora



En la gráfica anterior podemos identificar todos los dispositivos inalámbricos con que cuenta la red inalámbrica dentro del área de cobertura donde se hicieron las prácticas procurando siempre de que exista el mayor número de equipos que garanticen nuestra investigación.

Gráfico 3.8: Porcentaje de la Intensidad de la Señal
Fuente: La investigadora

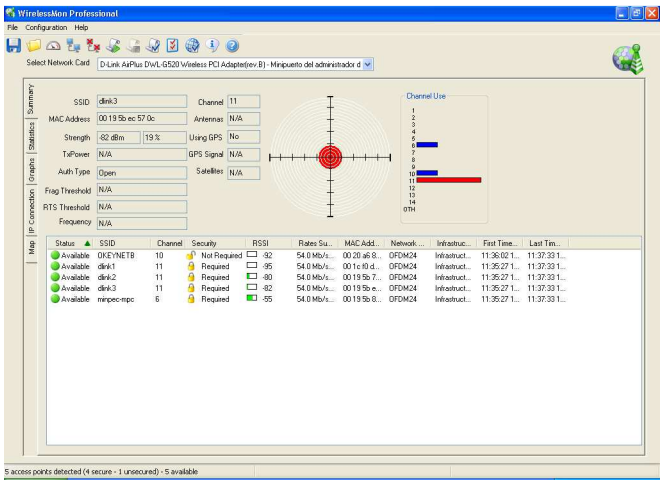


Wirelessmon

Con este software podemos ver las redes inalámbricas que están dentro del alcance de nuestra antena de la tarjeta de red inalámbrica.

En este grafico se muetra la señal de intensida de cada uno los acces point que nuestra tarjeta de red inalambrica puede capatr o estan al alance en el mismo que esta habilitadoi el SSID (minpec-mpc) para que todas las personas puedan ver el nombre de nuestro Access Point.

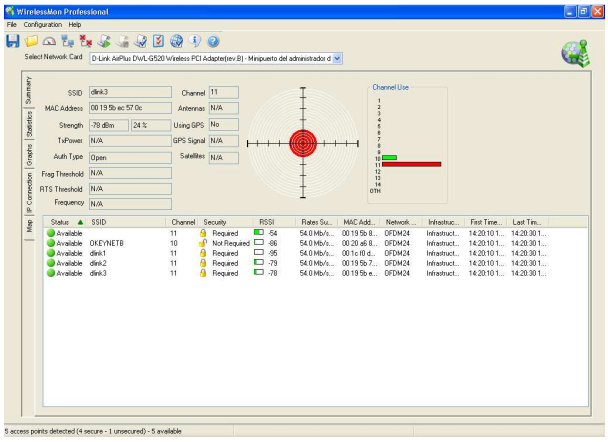
Gráfico 3.9: Habilitación del SSID
Fuente: La Investigadora



En este otro grafico esta deshabilitado el SSID (tesis o tannia) que son los ssid que se utilizó para estas prácticas aunque en ocasiones captura el de la institución donde se realizaron las pruebas de los equipos y el punto de acceso mediante computadora personal

Gráfico 3.10: Deshabilitar del SSID

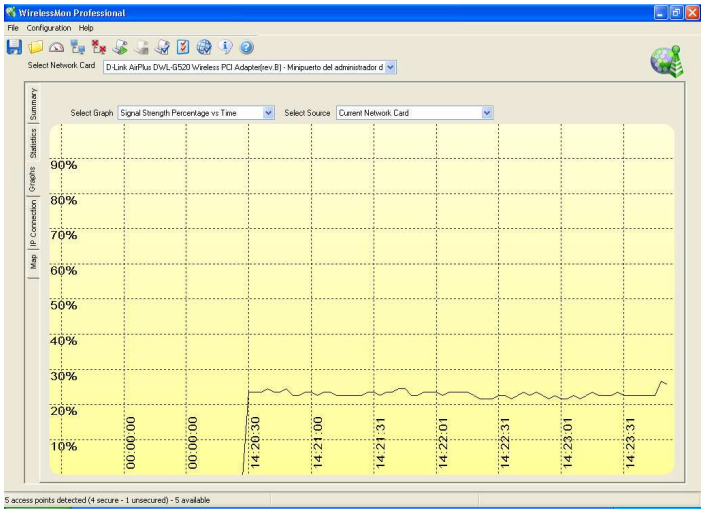
Fuente: La Investigadora



En este otro mostramos la representación gráfica de intensidad de señal conectada al Access Point Dlink3.

Gráfico 3.11: Intensidad de la Señal

Fuente: La Investigadora

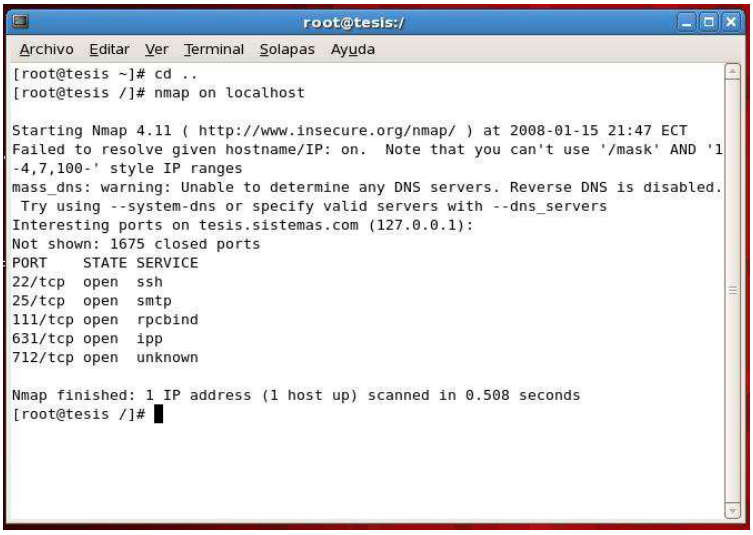


3.7.2. Configuración Servidor Proxy

Para la configuración del servidor proxy para poder repartir el recurso del internet debemos proceder habilitar el servicio del demonio SQUID el mismo que se encuentra dentro de los servicios etiquetados como bin en el directorio raíz del Linux CentOS.

Gráfico 3.12: Rastreos de puertos abiertos sin proxy.

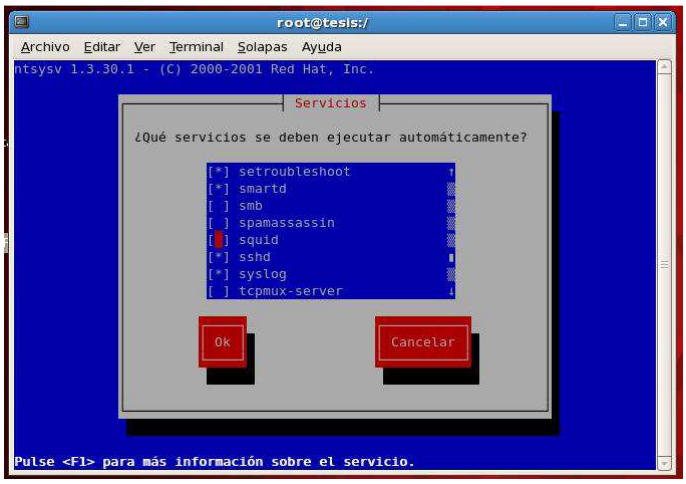
Fuente: La Investigadora



En la gráfica anterior podemos ver todos los servicios que se encuentran activos previo a poder subir el servicio de proxy en el que constan solo los necesarios sin ni siquiera necesitar las comunicaciones dentro de la red ni administración localizada.

Gráfico 3.13: Configuración de demonios en Linux.

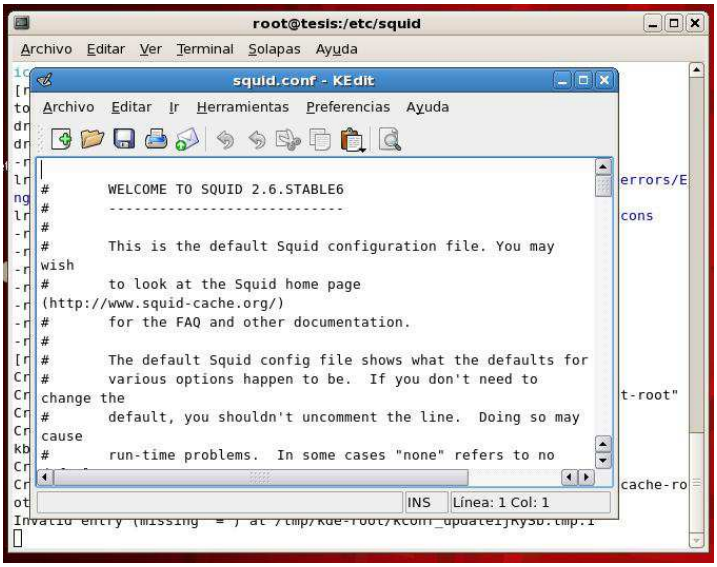
Fuente: La Investigadora



Esta es la manera como se administra los demonios en el servidor de Linux Centos , en el cual se debe activar y luego reiniciar el servicio para que entre en funcionamiento, claro luego de utilizar las reglas necesarias de filtrado o de administración remota.

Gráfico 3.14: Configuración del proxy (Squid)

Fuente: La Investigadora



Las reglas de configuración de los servicios se los debe ingresar y habilitar en los archivos .conf los cuales son los que contienen todas las reglas que se necesitan conocer dentro de la administración.

Este proceso se lo debe realizar en todos los archivos de configuración tales como el httpd para el apache y el iptable.rc.conf para lo que es el firewall según las reglas pre establecidas.

3.7.3 Firewalls

El hecho de disponer de una conexión a Internet puede ser causa de multitud de ataques a nuestro ordenador desde el exterior. Cuanto más tiempo permanezcamos conectado mayor es la probabilidad de que la seguridad de nuestro sistema se vea comprometida por un atacante desconocido.

Tan propio del espíritu comercial anglosajón, se designa a una utilidad informática que se encarga de aislar redes o sistemas informáticos respecto de otros sistemas informáticos que se encuentran en la misma red. Constituyen una especie de “barrera lógica” delante de nuestros sistemas que examina todos y cada uno de los paquetes de información que tratan de atravesarla. En función de unos criterios establecidos previamente deciden qué paquetes deben pasar y cuáles deben ser bloqueados. Muchos

son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los troyanos sean efectivos. En la figura se muestra gráficamente el concepto. El Firewall actúa de intermediario entre nuestra red local (o nuestro ordenador) e Internet, filtrando el tráfico que pasa por él.

Un Firewall, como se ha dicho, intercepta todos y cada uno de los paquetes destinados a o procedentes de nuestro ordenador, y lo hace antes de que ningún otro servicio los pueda recibir. De esto extraemos la conclusión de que el Firewall puede controlar de manera exhaustiva todas las comunicaciones de un sistema a través de Internet.

Otra función útil de la mayoría de los Firewall es su capacidad para mantener un registro detallado de todo el tráfico e intentos de conexión que se han producido (lo que se conoce como un Log). Estudiando los Log es posible determinar los orígenes de posibles ataques, descubrir patrones de comunicación que identifican ciertos programas malignos (lo que se conoce como Malware), etc... Sólo los usuarios avanzados podrán sacar partido a estos registros, pero es una característica que se le puede exigir perfectamente a estas aplicaciones.

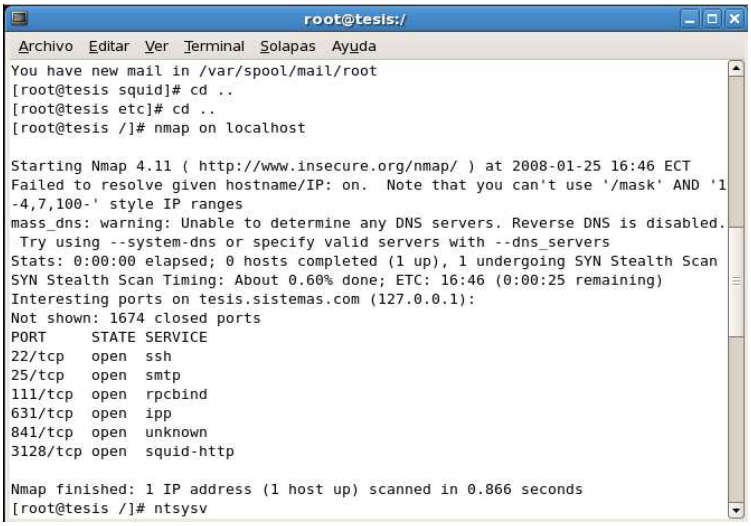
```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl Red src 192.168.0.0/255.255.255.0
#Sitios denegados
acl negados url_regex "/etc/squid/sitios-denegados"
#Autentificacion de usuarios
```

```
#acl password proxy_auth REQUIRED
#  TAG: http_access
#      Allowing or Denying access based on defined access lists
#
#      Access to the HTTP port:
#      http_access allow|deny [!]aclname ...
#
#      NOTE on default values:
#
#      If there are no "access" lines present, the default is to deny
#      the request.
#
#      If none of the "access" lines cause a match, the default is the
#      opposite of the last line in the list.  If the last line was
#      deny, then the default is allow.  Conversely, if the last line
#      is allow, the default will be deny.  For these reasons, it is a
#      good idea to have an "deny all" or "allow all" entry at the end
#      of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
```

En la parte superior se encuentra el código para el iptable el mismo que registra las restricciones para sitios prohibidos mediante un archivo el mismo que debe estar dentro del mismo directorio donde se encuentra los archivos de configuraciones como son: iptables.rc, iptables.rc1, una vez que tenemos todos los servicios arriba procedemos nuevamente a realizar un escaneo de puertos abiertos para ver cómo se encuentra configuradas las redes:

Gráfico 3.15: Rastreo de puertos con el proxy y el fireweall activados

Fuente: La Investigadora



Podemos observar que la red se encuentra habilitando el puerto 3128 que es el que asigna Linux al squid para el proxy que a diferencia de Windows 2003 y lo que es Microsoft es el puerto 80 o 8080.

Cabe anotar que siempre que los servicios estén bien subidos el punto de acceso no presentara ningún tipo de problemas por cuanto el servicios de squid como de apache y el de iptables el uno es complemento de otro y no se puede interferir en ningún caso con las actividades que cada cual desempeña.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Las redes inalámbricas están tomando mucha importancia en las actividades institucionales de hoy en día. Para lograr ser competitivos se requiere tener un acceso a la información desde cualquier sitio y temas de investigación como este son un aporte para las nuevas generaciones de ingenieros en sistemas

2. La velocidad de las redes inalámbricas es satisfactoria cuando se trata de transmisión y acceso a archivos de datos. Esto no sucede cuando se trata de transferencia de imágenes o videos según las pruebas realizadas.

3. Las seguridades dentro de las redes inalámbricas, al igual que una red cableada, tiene sus desventajas, pero actualmente se están estudiando mejoras para efectivizarlas y dar confianza a los usuarios de la misma.

4. Una red inalámbrica bien configurada, es tan eficiente como una red cableada. Pues podemos tener una comunicación de datos en tiempo real y seguro.

5. Si el diseño no es correcto al configurar e implantar una red inalámbrica, se puede interferir en otra red inalámbrica cercana.

6. Una red inalámbrica es más útil en una Organización, que en una red casera, pues sus costos en la actualidad, no son muy accesibles para el hogar y más aún cuando se utiliza una computadora que se va a dedicar a repartir el recurso del internet y en un sistema operativo muy poco difundido.

7. Los costos de mantenimiento en una red inalámbrica, son menores que los costos de una red cableada; ya que en una red cableada cualquier

remodelamiento de un espacio físico contribuye al incremento de gastos.

8. Se debe tomar siempre en cuenta los estándares y normas internacionales, tales como el de la IEEE 802.11 a, b, g para la configuración y administración de ciertos servicios con que cuentan los servidores, ya que de esta manera estaremos precautelando la información que se genera en los distintos departamentos.

9. El continuo avance de las tecnologías ha influenciado notablemente en la reestructuración de los estándares de la IEEE con la aparición de nuevos y mejores como es el caso del 802.11 min y de las normas ISO 27001 y 27001 dentro de estos se ha implementado el Código de Práctica para la Administración de la Seguridad de la Información.

10. La autoeducación en estudiantes de ingeniería en sistemas se la debe inculcar a todo nivel toda vez es importante que conozcan de nuevas tecnologías de la información y las comunicaciones.

RECOMENDACIONES

1. Se recomienda realizar mayores estudios sobre redes inalámbricas de parte de la Universidad Técnica de Cotopaxi a través de la Carrera de Ciencias de la Ingeniería y Aplicadas, ya que es una tecnología que avanza cada vez más en las empresas de renombre mundial.

2. Al utilizar redes inalámbricas, se recomienda que estas sean utilizadas para transferencias y acceso a archivos de datos, pues por el momento, es en este punto donde denota su mayor utilidad.

3. Se recomienda utilizar redes inalámbricas en medios en los que continuamente se realizan cambios de infraestructura dentro de un edificio, pues su costo a la larga es mucho más conveniente.

4. Se debe realizar un análisis de diseño antes de implementar una red inalámbrica, pues de su buen diseño y configuración depende de que no interfiera en otras redes cercanas.

5. Para un correcto y eficaz funcionamiento, se recomienda utilizar tecnología inalámbrica en Equipos con procesador de 5OOMhz o superior, 256 MB de memoria RAM o superior, Sistema Operativo Windows XP o superior.

6. Hay que manejarlas con mucha prudencia, ya que son herramientas que ayudan a la configuración de equipos hijos, tomando las características de la maquina host y mermando el rendimiento de ésta.

7. La adquisición de equipos sean estos servidores o equipos personales se lo debe realizar buscando cumplir con las expectativas de la empresa o institución donde se vaya a implementar la red inalámbrica.

8. Los estándares aplicados en este proyecto de tesis están siempre en actualización

por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la institución donde se lo implemente para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.

9. Se recomienda la capacitación en el manejo responsable de las redes inalámbricas que en la actualidad se encuentra implementado en la Universidad Técnica de Cotopaxi, conocer sus bondades así como sus deficiencias ya que todavía se tiene algunos altibajos

10. Para evitar conflictos de incompatibilidad de equipos de red y otros problemas se recomienda se tome como política de equipos con recursos suficientes a fin de evitarnos contratiempos en las configuraciones.

GLOSARIO DE TÉRMINOS Y SIGLAS

Acceso Físico

Es el medio utilizado para obtener información de las oficinas, salas de cómputo, escritorios y archivos.

Acceso Lógico

Es el medio utilizado para obtener información de las bases de datos y sistemas de información de la organización.

Activos

Son los recursos de la organización. Existen varios tipos de activos como son: Los recursos de información (bases de datos, los documentos de sistemas), los recursos de software (software de sistemas operativos, herramientas de desarrollo), activos físicos (equipamiento informático, equipos de comunicaciones, otros) y servicios (iluminación, energía eléctrica, etc.)

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Anomalía

Irregularidad en el funcionamiento de un sistema, de un software, de un control, etc.

Camino Forzado

Ruta limitada entre una Terminal de usuario y los servicios del computador. Evita que los usuarios seleccionen rutas fuera de la trazada entre su Terminal y los servicios a los cuales está autorizado a acceder.

Canal Oculto

Es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que a priori no estaría autorizado a acceder a dicha información.

Clave Pública

Clave que puede ser revelada a cualquier persona.

Clave Secreta

Clave que debe mantenerse en secreto.

Código Troyano

Es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.

Comercio Electrónico

Consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas.

Computación Móvil

Se define como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

Criptografía

Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que sólo puedan ser leídos por la persona que posee la clave de descodificación.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.

Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

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. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Evaluación de Riesgos

Es un proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse. La evaluación de riesgos consta de una fase llamada de análisis de riesgos (identificación de peligros y estimación de los riesgos) y una fase posterior de valoración de riesgos y de control de riesgos si fuese posible.

Evidencia

Datos, registros, declaraciones de hecho o cualquier otra información que respaldan la existencia o veracidad de algo.

HONEYPOTS (Tarro de Miel)

Recurso de red destinado a ser atacado o comprometido. Los Honeypots son los encargados de proporcionar información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales. Es decir el objetivo de los Honeypots es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.

HONEYNETS (Tarro de Miel)

Es un tipo de Honeypot. Específicamente es un Honeypot altamente interactivo diseñado para la investigación y la obtención de información sobre atacantes. Un Honeynet es una arquitectura, no un producto concreto o un software determinado. Y consiste no en falsear datos o engañar a un posible atacante (como suelen hacer algunos Honeypot), sino que el objetivo principal es recoger información real de cómo actúan los atacantes en un entorno de verdad.

Incidente

Dícese del fallo que sucede en un equipo o sistema de manera temporal o aleatoria, sin que existan unos motivos claros para ello.

Procesamiento de Información

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.
Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

Seguridad Informática

Conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la perdida física de datos.

Seguridad de la Información

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información. La seguridad de la información es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Servicio de Información

Un servicio para los sistemas que proporciona un sistema de base de datos para los archivos de configuración comunes.

Servicio de Red

Es un servicio para que cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes.

Sistema de Información

Conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sistema Informático

Es aquel sistema que se encarga del manejo de información en la computadora, a través de la cual el usuario controla las operaciones que realiza el procesador.

Sistema Operativo

Termino que se utiliza para referirse al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Software Malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

Trabajo Remoto

Se refiere al trabajo que una persona realiza por fuera de su puesto de trabajo normal.

Utilitarios del Sistema

Reconstruir índices, compactar y validar bases de datos, validar consistencia de datos, cambiar fecha de operación y del sistema, importar y exportar datos entre

empresas, transferir productos, precios, existencias de almacén y acceso al generador de reportes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps

Fast Ethernet 100 Mbps

Gigabit Ethernet 1000 Mbps

4.4.- BIBLIOGRAFÍA

- **Andrew Tanenbaum,** Redes de Computadores, Cuarta Edición 2004
- **Tyson Creer,** Así son las Intranets, Segunda Edición. 2002
- Building Cisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.
- **VLADIMIROV ANDREW A. (2005)**, Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.
- **ANSI/IEEE STD 802.11, 1999** Edition. [1]"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.

4.4.1. - WEB BIBLIOGRAFÍA

- http://www.linuxparatodos.com/honeypot.htm
- http://www.linuxparatodos.com/ids.htm
- http://www.linuxparatodos.com/ips.htm
- http://lauca.usach.cl/~lsanchez/Vlan/
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- http://www.avantel.net/~rcruz/Cap3qosrba.pdf
- http://www.lavioleta.net/Capitulo1.htm

- http://www.commlogik.com.ar/cisco.html
- http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario
- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf
- http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf
- http://net21.ucdavis.edu/newvlan.htm
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf
- http://www.emagister.com/frame.cfm?id_user=88930200502696748506748707 04555&id_centro=57953030052957564866666952674548&id_curso=65425040 05016755545768550674555&url_frame=http://www.emagister.com/public/pdf /comunidad_emagister/017931200431686948496770654845 67-config-ciscos.pdf
- http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf
- http://www.isa.uniovi.es/docencia/redes/tema4.pdf
- http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20suppo rt%20MM%20apps.pdf
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf
- http://www.adictosaltrabajo.com/linux/proxy.htm
- http://www.adictosaltrabajo.com/linux/proxyinverso.htm
- http://www.adictosaltrabajo.com/linux/firewall.htm
- http://www.adictosaltrabajo.com/linux/cortafuegos.htm
- http://www.monografias.com/proxy.htm
- http://www.monografias.com/firewall.htm
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf

- http://www.si.uji.es/bin/ponencies/ipp.pdf
- http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf
- http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm