UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

SEGURIDAD EN REDES WI-FI

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

ALFREDO CERVANTES GONZÁLEZ

ASESOR: I.M.E. OSCAR HERNÁNDEZ SÁNCHEZ

CUAUTITLÁN IZCALLI, EDO. DE MÉX. 2015

VNIVERSIDAD NACIONAL AVPNPMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
UNIDAD DE ADMINISTRACIÓN ESCOLAR
DEPARTAMENTO DE EXÁMENES PROFESIONALES

ASUNTO: VOTO APROBATORIO

M. en C. JORGE ALFREDO CUÉLLAR ORDAZ
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: M. en A. ISMAEL HERNANDEZ MAURICIO
Jefe del Departamento de Examenes
Profesionales de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos a comunicar a usted que revisamos **La Tesis:**

SEGURIDAD EN REDES WI-FI

Que presenta el pasante: ALFREDO CERVANTES GONZALEZ
Con número de cuenta: 30508719-3 para obtener el Título de: **Licenciado en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**

ATENTAMENTE
"POR MIRAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 27 de Enero del 2015.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	M.A.I. Manuel Jauregui Renault	
VOCAL	I.M.E. Oscar Hernández Sánchez	
SECRETARIO	M.A. Jacqueline Valadez Romero	
1er SUPLENTE	I.M.E. José Juan Rico Castro	
2do SUPLENTE	L.I. Rosalba Nancy Rosas Fonseca	

DEDICATORIA

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, porque creyeron en mí y porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, por motivarme y darme la mano cuando sentía que el camino se terminaba y porque el orgullo que sienten por mí, fue lo que me hizo ir hasta el final, a ustedes por siempre mi corazón, mi amor y mi agradecimiento.

Papá, Mamá y Hermano

AGRADECIMIENTOS

A mi Madre

Por su apoyo incondicional, por estar siempre a mi lado en todo momento bueno o malo, por haberme enseñado los buenos valores, haberme dado sus mejores consejos y por todo su amor. Que esto sea parte de la recompensa por todos estos años de entrega, desvelos y apoyo. Te quiero con todo mi corazón.

A mi padre

Por sus largas platicas de enseñanza y sus buenos consejos que lo caracterizan, por todos los días que me preguntabas como me había ido, por tu amor, confianza y apoyo. Detrás de este gran logro estas tú, gracias por darme la oportunidad de realizar este sueño compartido y porque un peón tuyo al fin se corono. Te amo y siempre te amaré.

A mi hermano

Por ser una persona importante en mi vida, por el apoyo brindado hacia este trabajo, por los mejores momentos de nuestras vidas y por hacerme reír en momentos de tristeza y siempre animarme, gracias por tu cariño. Te quiero enano. Siempre contaras conmigo.

AGRADECIMIENTOS

A mis Tíos y Abuelos

Por ser una gran fuente de apoyo en todo momento de mi vida y por sus buenos consejos y enseñanzas. Gracias a ustedes!

A mis profesores

A quienes les agradezco por sus enseñanzas, su paciencia y su apoyo en todo momento de mi carrera. Gracias a todos!

Índice

Índice de Ilustraciones

Índice de Tablas

Nota: Las ilustraciones aquí presentadas son únicamente con fines ilustrativos, y fueron capturadas con el uso del Sistema Operativo Windows 7® y la distribución de GNU/Linux® Backtrack 5, respetando los derechos de los autores y de sus programadores.

Introducción

Las redes inalámbricas se han convertido en una alternativa muy accesible e interesante a diferencia de las redes cableadas. Esto se debe a su bajo costo, facilidad de instalación y la libertad que ofrecen para poder conectarse en cualquier lugar, ya que, podemos transferir información de una habitación a otra o de una oficina a otra sin ningún cable, estos son algunos que han beneficiado el crecimiento de eta tecnología, hoy en día se ocupa en salas de conferencias, en universidades, en bibliotecas, en un almacén, en el auto, desde casa, en la escuela, en el aeropuerto, en el hotel, en la cafetería, en oficinas , etcétera.

Estas redes están basadas en estándares implementados por diversos organismos tales como IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), mencionado en este trabajo, han estado hasta hace poco relegadas a entornos de escasos metros cuadrados.

Un panorama que ha cambiado radicalmente con la inminente aparición de las nuevas tecnologías, capaces de ofrecer conexiones de banda ancha alcanzando distancias hasta de 50 km y algunas de ellas con distancias a nivel mundial.

Sin embargo esta tecnología inalámbrica con todo y sus ventajas conlleva una contraparte muy importante en cuestión de problemas de seguridad, este tipo de problemas se han dado a conocer no solo por los administradores de la red, sino también de los usuarios de la misma. A estas alturas está demostrado que las redes inalámbricas no son del todo seguras y que es necesario un importante avance en cuestiones de seguridad.

Parte de los objetivos de este trabajo es dar a conocer las características y/o técnicas a nivel de seguridad de los estándares y dispositivos más usados en la actualidad en el hogar y pequeñas empresas. Dar a conocer los ataques más comunes usando tecnologías de infiltración y de acceso de fuerza bruta a los que se enfrentan este tipo de redes en la actualidad.

Este trabajo no pretende ser exhaustivo ni abarcar todos los ataques y sus variantes, solo dar a conocer de manera simple y entendible el funcionamiento de estos ataques y dar una solución a los mismos.

Como se ha mencionado las redes inalámbricas no son del todo seguras, por este motivo se darán a conocer medidas de seguridad en específico de una red inalámbrica tanto en sus dispositivos como en las AP (Access Point) y de esta forma mantener nuestra red con la mayor seguridad posible protegiendo nuestra privacidad e información que estemos manejando.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas ya que estas ofrecen velocidades de transmisión aún. Mientras que las redes inalámbricas actuales ofrecen velocidades de 6 Mbps en hogares y en pequeñas empresas ofrecen conexiones de hasta 100 Mbps; las redes cableadas ofrecen velocidades de 10 Mbps hasta 10 Gbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores.

Los avances tecnológicos son cada vez mayores al igual que la demanda de sistemas y redes, esto da pauta a un continuo mejoramiento de las redes inalámbricas en cuestiones de seguridad y rapidez, ya que son una herramienta indispensable e importante en la actualidad en cualquier ámbito de trabajo y del hogar.

Justificación

El desarrollo sobre el área de la seguridad Wireless Fidelity (WI-FI) es un tema muy importante, dentro de las tecnologías de la comunicación, ya que hoy en día es una necesidad muy grande que esta implementación sea la adecuada. El tema de la seguridad debe de ser estandarizado totalmente ya que es de vital importancia para todos el garantizar la fiabilidad en el manejo de la información de manera uniforme.

Es por esta razón que se hace muy importante investigar a fondo los problemas que están emergiendo diariamente en seguridad en redes inalámbricas, como esto es un tema de permanente evolución, se dice que a medida que aumenta la tecnología el nivel de seguridad debe de ser más grande por las facilidades que los delincuentes encuentran para romperla debemos evitarlo con mejoras sustanciales.

Relevancia social: ¿cuál es su relevancia para nuestra sociedad?, ¿quiénes se beneficiarán con los resultados de la investigación?, ¿de qué modo?, ¿qué proyección social tiene?

Actualmente en México se está presentando un proceso de transición en la tecnología, lo que hace que las redes de telecomunicaciones sean de más importancia cada día debido a que en particular se presenta la necesidad de aplicar tecnologías de redes inalámbricas, lo que por consecuencia trae consigo la necesidad de hacer aportes que ayuden a mejorar la seguridad, tanto a las redes de comunicación directamente, así como implementar organismos que vigilen y regulen el funcionamiento de estas.

Para esto es necesario crear e implementar nuevos estándares que aseguren la compatibilidad en el mercado nacional, para así promover el uso de estas cubriendo las necesidades de la población.

Objetivo general

Describir las tendencias de las tecnologías en seguridad más comerciales de redes inalámbricas y dar un panorama más general sobre las ventajas de utilizar e implementar protocolos de redes Wi-Fi en el hogar y pequeñas empresas.

Objetivos específicos

- Explicar de manera sencilla cómo es que funcionan este tipo de redes inalámbricas y la diferencia entre las distintas señales (WEP, WPA, WPA2).

- Describir algunos de los métodos más comunes para infligir en este tipo de redes inalámbricas ocupando ciertos tipos de programas con una pequeña explicación.

- Explicar de manera entendible que es lo que están haciendo algunos de los fabricantes líderes para dar más seguridad en este tipo de redes inalámbricas y dar una noción de cuál es la tendencia en las mismas.

- Dar a conocer las familias de las normas IEEE 802 y 802.11.

- Proponer estrategia para mantener seguras las redes inalámbricas, mediante algunas configuraciones en nuestros equipos de red y buenas prácticas de uso.

Capítulo 1

1.0 Antecedentes

En la década de 1940, los computadores eran enormes dispositivos electromecánicos que eran propensos a sufrir fallas. En 1947, la invención del transistor semiconductor permitió la creación de computadores más pequeños y confiables. En la década de 1950 los computadores mainframe, que funcionaban con programas en tarjetas perforadas, comenzaron a ser utilizados habitualmente por las grandes instituciones.

A fines de esta década, se creó el circuito integrado, que combinaba muchos y, en la actualidad, millones de transistores en un pequeño semiconductor. En la década de 1960, los mainframes con terminales eran comunes, y los circuitos integrados comenzaron a ser utilizados de forma generalizada.

En esa misma década solamente existían unas cuantas computadoras aisladas. El usuario tenía que estar cerca de la computadora porque los terminales, los únicos mecanismos de acceso a la computadora, estaban conectados mediante un cable.

Hacia fines de la década de 1960 y durante la década de 1970, se inventaron computadores más pequeños, denominados minicomputadores. Sin embargo, estos minicomputadores seguían siendo muy voluminosos en comparación con los estándares modernos.

En 1977, la Apple Computer Company presentó el microcomputador, conocido también como computador personal.

En 1981 IBM presentó su primer computador personal. El equipo Mac, de uso sencillo, el PC IBM de arquitectura abierta y el posterior micro miniaturización de los circuitos integrados dio como resultado el uso difundido de los computadores personales en hogares y empresas.

A mediados de la década de 1980 los usuarios con computadores autónomos comenzaron a usar módems para conectarse con otros computadores y compartir archivos. Estas comunicaciones se denominaban comunicaciones punto-a-punto o de acceso telefónico. El concepto se expandió a través del uso de computadores que funcionaban como punto central de comunicación en una conexión de acceso telefónico.

Estos computadores se denominaron tableros de boletín. Los usuarios se conectaban a los tableros de boletín, donde depositaban y levantaban mensajes, además de cargar y descargar archivos. La desventaja de este tipo de sistema era que había poca comunicación directa, y únicamente con quienes conocían el tablero de boletín.

Otra limitación era la necesidad de un módem por cada conexión al computador del tablero de boletín. Si cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco líneas telefónicas diferentes.

A partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos (DoD) desarrolló redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico. Esta tecnología era diferente de la comunicación punto-a-punto usada por los tableros de boletín.

Esta tecnología permitía el internet working de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión. La WAN del DoD finalmente se convirtió en la Internet.

La primera red informática surgió en la Guerra Fría en 1957 cuando los Estados Unidos crearon la Advanced Research Projects Agency Network (ARPANET), fue creada durante la cortina de hierro, y su objetivo principal era que la información militar de los Estados Unidos no estuviera centralizada y pudiera estar disponible en punto del país ante un eventual ataque ruso. Ver ilustración 1.

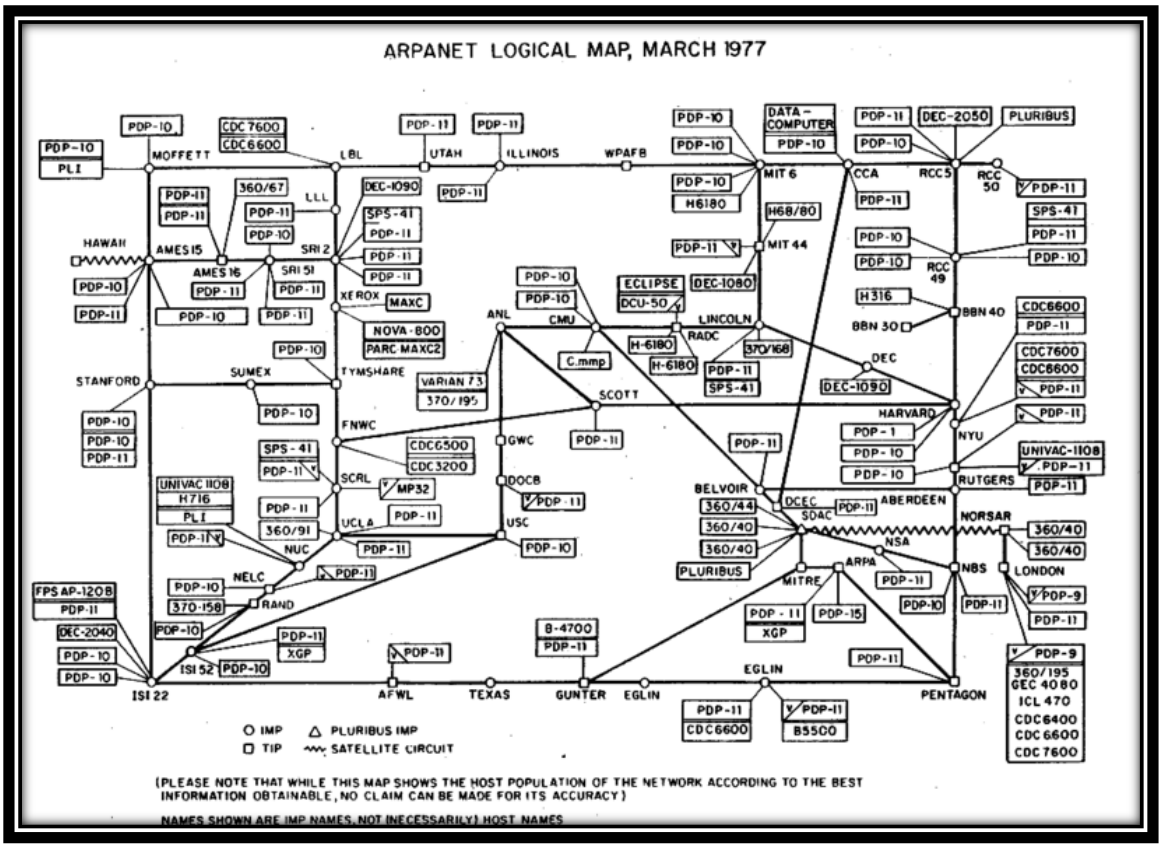

Ilustración 1 Mapa Lógico de ARPANET

The Computer History Museum, en:File:Arpnet-map-march-1977.png, ARPANET, 1977

Posteriormente a la creación de ARPANET, Leonard Kleinrock, un investigador de Massachusetts Institute of Technology (MIT), escribía el primer libro sobre tecnologías basadas en la trasmisión de un mismo cable de más de una comunicación.

En 1965, la Arpanet patrocino un programa que trataba de analizar las redes de computación usando computadoras. Mediante este programa la maquina TX-2 en el laboratorio Lincoln del MIT y la AN/FSQ32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea delicada de 1200 bits por segundo.

En 1968 la ARPANET no espera más y llama a empresas y universidades para que propusieran diseños, con el objetivo de construir la futura red. La universidad de california gana la propuesta para el diseño de gestión de red y la empresa BNN (Bold Beraneck and Newman Inc.), gana el curso de adjudicación para el desarrollo de la tecnología de conmutación de paquetes mediante la implementación de la Interface Message Processors (IMP).

En 1969, se establece la primera conexión de ARPANET, comienza a utilizar para sus primeras comunicaciones un protocolo Host-to-host. Este protocolo se denomina NCP y es el antecesor del actual TCP/IP que se utiliza en toda la internet. Esta primera conexión estaba conformada por 4 nodos las cuales eran minicomputadoras Honeywell DDP-516 con 12k en memoria con líneas telefónicas con 50 kbps. Los cuatro nodos estaban situados en:

- UCLA (Universidad de California en Los Angeles).
- SRI (Stanford Research Institute).
- UCBS (Universidad de California de Santa Bárbara, Los Angeles).
- La Universidad de UTA.

La primera comunicación entre 2 computadores se produce entre UCLA y Stanford el 20 de octubre de 1969. El autor de este envío fue Charles Kline de UCLA.

No fue hasta 1971 cuando un grupo de investigadores bajo la dirección de Norman Abramson, en la Universidad de Hawaii, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Ver ilustración 2.

Ésta es la primera red de área local inalámbrica (WLAN), estaba formada por 7 computadoras situadas en distintas islas que se podían comunicar con un ordenador central al cual pedían que realizara cálculos. Uno de los primeros problemas que tuvieron y que tiene todo nuevo tipo de red inventada fue el Control de Acceso al Medio (MAC), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí.

En un principio se solucionó haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras mientras estuviera libre, de tal forma que cuando una de las otras estaciones se disponía a transmitir, antes “escuchaba” y se cercioraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, esto se conoce como Carrier Sense Multiple Access (CSMA).

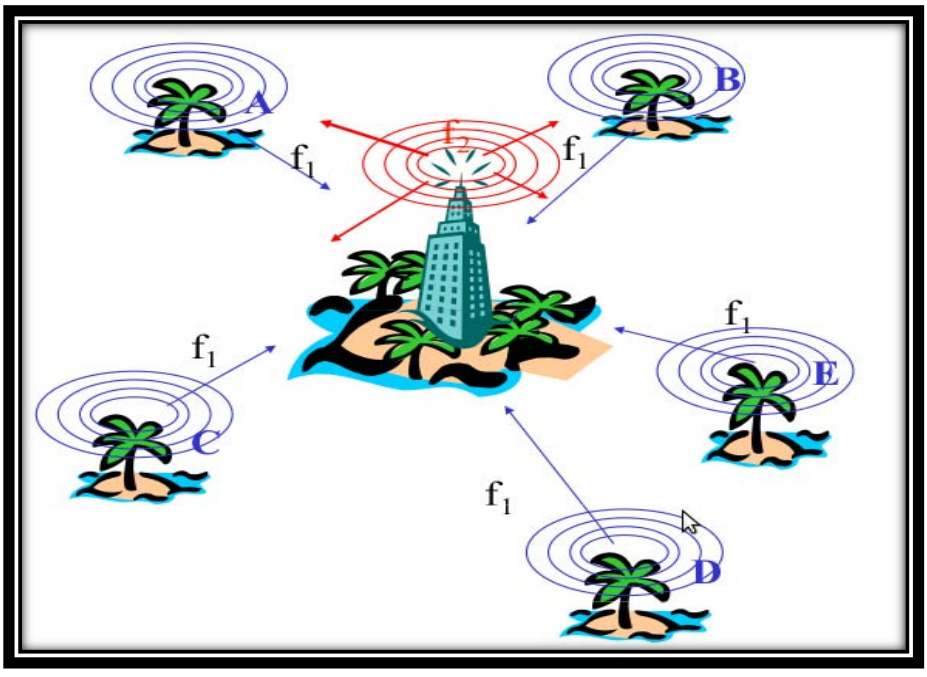

Ilustración 2 Red ALOHA

Un año después ALOHA se conectó mediante ARPANET al continente americano. ARPANET es una red de computadoras creada por el Departamento de Defensa de los EEUU como medio de comunicación para los diferentes organismos del país.

A finales de la década de los setenta se publicaron los resultados de un experimento consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica llevada a cabo por IBM en Suiza.

En 1983, Paul Mockapetris y Jon Postel crearon el Sistema de Nombres de Dominio (DNS) y las denominaciones .com, .org, y .gov, tan características de lo que hoy llamamos Internet.

La última etapa en el desarrollo fue la creación de la World Wide Web (WWW), a cargo de Tim Berners-Lee, quien a principio de los ’90 inventó el sistema de links, fundamental para el crecimiento de la red de redes. Tim Berners no patentó su invento para no poner escollos comerciales a la evolución de Internet. Su aporte fue reconocido recientemente, cuando fue condecorado como caballero por la realeza británica y además fue elegido por la revista Time como uno de los 20 pensadores más influyentes del siglo XX.

De todos modos, aunque no haya consenso total sobre cuál fue el hecho que le dio origen a lo que hoy conocemos como Internet, es indudable que aquella primera red ARPANET, que nació hace 57 años, fue fundamental para el inicio de lo que hoy podemos llamar simplemente “La Red”.

1.1 Conceptos Básicos

Para hacer un poco más entendible el concepto de redes olvidémonos de la informática por un minuto, llamamos en general Red, a un conjunto de elementos unidos entre sí mediante algún medio. Ejemplo las Ciudades de un País se unen mediante las carreteras, o las vías del tren, que van uniendo unas ciudades con otras.

Entendido este concepto adentrémonos a la Informática, aquí llamamos red aun conjunto de computadoras o PC, más o menos potentes unidos por algún medio, básicamente el cable, o bien mediante dispositivos electrónicos de forma inalámbrica.

Dentro de la primera categoría, es decir unidas por cable, en principio comenzó utilizándose únicamente un tipo de cable para unir las distintas computadoras que formaban la red, este era el cable coaxial, compuesto por solo dos polos, un cable de un solo hilo llamado activo, aislado de una malla que lo recubría y que era conectado a masa.

Posteriormente comenzó a utilizarse el cable de par trenzado, en principio recubierto con una malla casi igual que la del anterior cable BNC, en este caso la malla solo tenía la finalidad de aislar de ruidos la señal que circulaba por los cables existentes en su interior. Este tipo de cable se ha ido sofisticando y adecuándose a las velocidades de transmisión necesaria, lo que dio paso a las llamadas categorías, categorías 3, 5, 5+ etcétera.

Más tarde se incorporó la red de conexión inalámbrica o Wireless Fidelity (WI-FI). Una conexión WiFi utiliza señales de radio, al igual que los teléfonos celulares y otros dispositivos similares. La tarjeta adaptadora inalámbrica de un equipo convierte los datos en señales de radio, que se transmiten por una antena.

Después, el Router recibe y decodifica estas señales de códigos binarios, para luego enviar la información a Internet, mediante una Local Area Network, Red de área local (LAN) o Ethernet por cable. Un servicio de la red Ethernet por cable puede ser una conexión de red por cable o por DSL.

1.1.1 Red de computadoras

También llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

1.1.2 Definición de Red y conceptos asociados

Cuando se habla de una Red, se entiende como un grupo de individuos que, en forma agrupada o individual, se relacionan con otros con un fin específico, caracterizado por la existencia de flujos de información. Las redes pueden tener muchos o pocos actores y una o más clases de relaciones entre pares de actores. Una Red se compone, por tanto, de tres elementos básicos los cuales son: nodos o actores, vínculos o relaciones y, flujos.

SSID Es el nombre de la red, todos los paquetes de información que se envían o reciben llevan esta información.

WEP Sistema de cifrado para redes WIFI, no es seguro, ya que han aparecido vulnerabilidades que provocan que se pueda saltar fácilmente.

WPA Sistema posterior a WEP que mejora notablemente la encriptación de WEP, aunque la versión definitiva es WPA2.

WPA2 Sistema de cifrado, evolución del WPA, con contraseña de 128 bits, se considera seguro.

IP Una dirección formada por una serie de números que identifica a nuestro equipo de forma unívoca dentro de una red.

MAC Es un valor que los fabricantes asignan a cada componente de una red, y que los identifica de forma unívoca, es como el DNI del dispositivo. Tienen dirección MAC las tarjetas de red, los routers, los USB WIFI... todos los dispositivos que puedan tener una IP.

1.1.3 DHCP

Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos de dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente.

1.1.4 NIC/MAU (Tarjeta de red)

NIC (Network Interface Card) o Tarjeta de Interfaz de Red también llamada MAU (Medium Access Unit) o Medio de Unidad de Acceso. Cada computadora necesita el “hardware” para transmitir y recibir información.

Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte trasera de la PC al cual se conecta el cable de la red.

Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas. A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base 5) o porque el medio sea distinto del que utiliza la tarjeta.

Hubs

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

Repetidores

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

Bridges

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo.

Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

Routers

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

Gateways

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

Módems

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras. Los módems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

1.2 Componentes básicos de una red

1.2.1 Servidor

Es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones. Puede ser dedicado o no dedicado. El sistema operativo de la red está cargado en el disco fijo del servidor, junto con las herramientas de administración del sistema y las utilidades del usuario.

Estaciones de Trabajo

Se pueden conectar a través de la placa de conexión de red y el cableado correspondiente. Los terminales ´tontos´ utilizados con las grandes computadoras y minicomputadoras son también utilizadas en las redes, y no poseen capacidad propia de procesamiento.

Sin embargo las estaciones de trabajo son, generalmente, sistemas inteligentes. Los terminales inteligentes son los que se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sea el equipo mejor.

Tarjetas de Conexión de Red

Permiten conectar el cableado entre servidores y estaciones de trabajo. En la actualidad existen numerosos tipos de placas que soportan distintos tipos de cables y topologías de red. Las placas contienen los protocolos y órdenes necesarios para soportar el tipo de red al que está destinada. Muchas tienen memoria adicional para almacenar temporalmente los paquetes de datos enviados y recibidos, mejorando el rendimiento de la red.

Cableado

Una vez que tenemos las estaciones de trabajo, el servidor y las placas de red, requerimos interconectar todo el conjunto. El tipo de cable utilizado depende de muchos factores, que se mencionarán a continuación. Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica. Además se pueden realizar conexiones a través de radio o microondas.

Cada tipo de cable o método tiene sus ventajas y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad. La velocidad y longitud del tendido son otros factores a tener en cuenta el tipo de cable a utilizar.

Par Trenzado: Consiste en dos hilos de cobre trenzado, aislados de forma independiente y trenzados entre sí. El par está cubierto por una capa aislante externa.

Cable Coaxial: Se compone de un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra. Entre el hilo conductor y la malla hay una capa gruesa de material aislante, y todo el conjunto está protegido por una cobertura externa.

Conexión fibra óptica: Esta conexión es cara, permite transmitir la información a gran velocidad e impide la intervención de las líneas. Como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctricas o emisión de señal. El cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta. La fibra está encapsulada en un cable protector.

1.2.2 Dispositivos de Comunicación Inalámbricos

Los componentes inalámbricos se utilizan para la conexión a redes en distancias que hacen que el uso de adaptadores de red y opciones de cableado estándares sea técnica o económicamente imposible. Las redes inalámbricas están formadas por componentes inalámbricos que se comunican con LAN.

Excepto por el hecho de que no es un cable quién conecta los equipos, una red inalámbrica típica funciona casi igual que una red con cables: se instala en cada equipo un adaptador de red inalámbrico con un transceptor (un dispositivo que transmite y recibe señales analógicas y digitales). Los usuarios se comunican con la red igual que si estuvieran utilizando un equipo con cables.

Transmisión por Infrarrojos

Funciona utilizando un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben; si hay algo que bloquee la señal infrarroja, puede impedir la comunicación.

Estos sistemas deben generar señales muy potentes, ya que las señales de transmisión débiles son susceptibles de recibir interferencias de fuentes de luz, como ventanas.

Transmisión vía Radio en Banda Estrecha

El usuario sintoniza el transmisor y el receptor a una determinada frecuencia. La radio en banda estrecha no requiere visibilidad directa porque utiliza ondas de radio.

Sin embargo la transmisión vía radio en banda estrecha está sujeta a interferencias de paredes de acero e influencias de carga. La radio en banda estrecha utiliza un servicio de suscripción. Los usuarios pagan una cuota por la transmisión de radio.

Capítulo 2

2.0 Redes de Computadoras

Red, es una estructura que dispone de un patrón característico. Una computadora u ordenador, por su parte, es una máquina electrónica que procesa datos y que posibilita la ejecución de distintas secuencias o rutinas indicadas por el usuario.

Una red de computadoras, por lo tanto, es un conjunto de estas máquinas donde cada uno de los integrantes comparte información, servicios y recursos con el otro. Por lo general se habla de red informática ya que es habitual que, además de las computadoras, se utilicen otros equipos complementarios para facilitar la comunicación (como un router o un switch).

La red de computadoras permite compartir recursos a distancia, aumenta la velocidad de la transmisión de datos (es más rápido acceder a un archivo por una red que a través de internet, por ejemplo) e incrementa la confiabilidad.

2.1 Protocolo

Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.

2.2 Modelo de referencia OSI

El modelo de interconexión de sistemas abiertos, también llamado Open System Interconnection (OSI). Ver ilustración 3.

Fue desarrollado en 1980 por la Organización Internacional de Estándares (ISO), una federación global de organizaciones que representa aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

El modelo especifica el protocolo que debe usarse en cada capa, y suele hablarse de modelo de referencia ya que se usa como una gran herramienta para la enseñanza de comunicación de redes.

Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran.

De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder comunicarse entre sí. Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet.

"El modelo OSI tiene 7 capas. Los principios que se aplicaron para llegar a las 7 capas se puedes resumir de la siguiente manera:

1.- Se debe crear una capa en donde se requiera un nivel diferente de abstracción.

2.- Cada capa debe realizar una función bien definida.

3.- La función de cada capa se debe elegir teniendo en cuenta la definición de protocolos estandarizados internacionalmente.

4.-Es necesario elegir los límites de las capas de modo que se minimice el flujo de información a través de las interfaces.

5.- La cantidad de capas debe ser suficiente como para no tener que agrupar funciones distintas en la misma capa; además, debe ser lo bastante pequeña como para que la arquitectura no se vuelva inmanejable." (Tanenbaum & Wetherall, 2012).

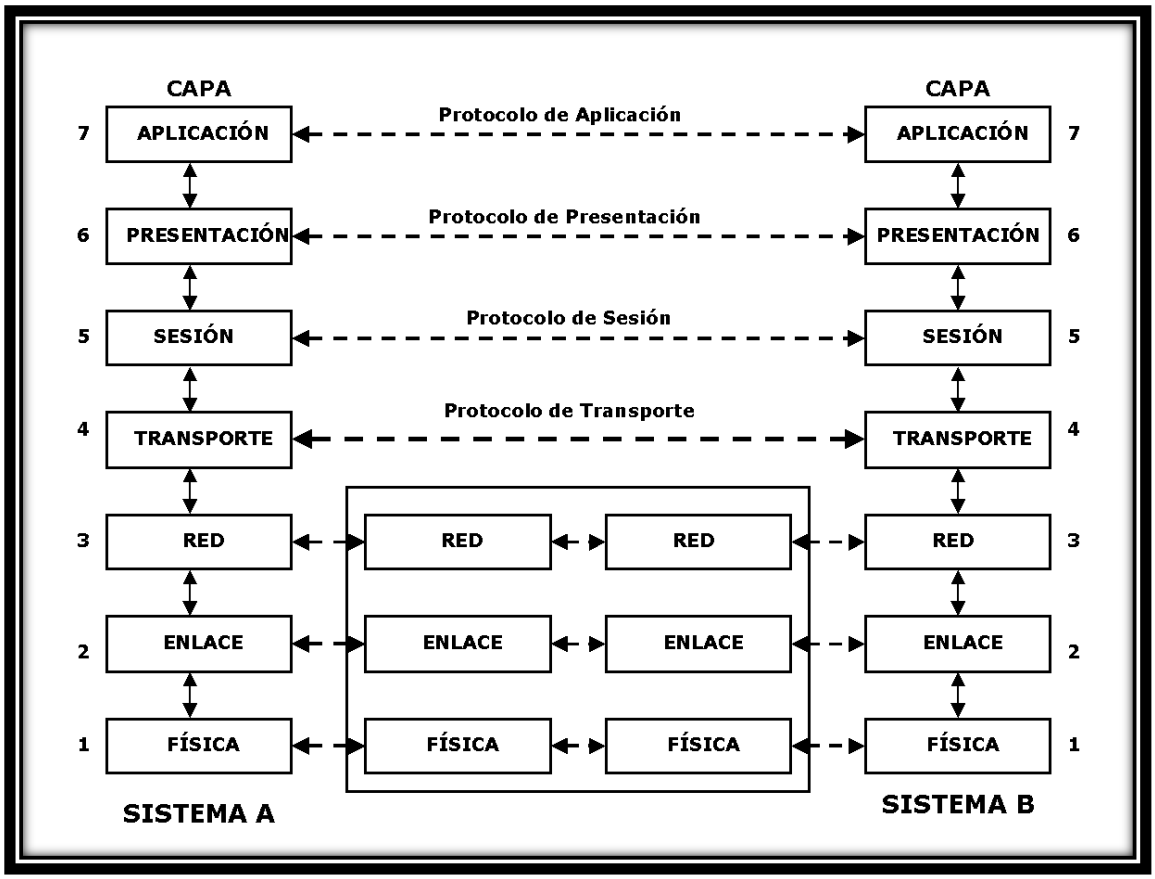

Ilustración 3 Modelo de referencia OSI

A continuación se dan a conocer de manera general cada capa del modelo en orden, empezando por la capa inferior. Teniendo en cuenta que el modelo OSI en sí no es una arquitectura de red, ya que no especifica los servicios y protocolos exactos que se van a utilizar en cada capa.

2.2.1 La capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos e integridad de los mismos, distancias de transmisión máximas, conectores físicos (cable coaxial, cable de par trenzado, fibra óptica, radio, microondas), características del medio (tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y otros atributos similares son definidos por las especificaciones de la capa física.

2.2.2 La capa de enlace de datos

La capa de enlace de datos es la responsable de la transferencia fiable de la información a través de un circuito de transmisión de datos. El objetivo de esta capa es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a conexión). Para lograr este objetivo tiene que montar bloques de información (llamados tramas en este nivel), si el servicio es confiable, para confirmar la recepción correcta de cada trama, el receptor devuelve una trama de confirmación de recepción.

Dotarles de una dirección de nivel de enlace, gestionar la detección o corrección de errores, y ocuparse del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento). Cuando el medio de comunicación está compartido entre más de dos equipos es necesario arbitrar el uso del mismo.

2.2.3 La capa de red

La capa de red es la que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

En esta capa pueden ocurrir ciertos errores, *"Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red puede ser distinto del que utiliza la primera. La segunda red tal vez no acepte el paquete debido a que es demasiado grande. Los protocolos pueden ser diferentes, etc. Es responsabilidad de la capa de red solucionar todos estos problemas para permitir la interconexión de rede heterogéneas."* (Tanenbaum & Wetherall, 2012).

2.2.4 La capa de transporte

La función básica de la capa de transporte es la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo.

La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina destino, independientemente de la red de redes física en uno.

"La capa de transporte también determina el tipo de servicio que debe proveer en la capa de sesión y, en última instancia a los usuarios de la red. El tipo más popular de conexión de transporte es un canal punto a punto libre de errores que entrega los mensajes o bits en el orden en el que se enviaron." (Tanenbaum & Wetherall, 2012).

De esta forma al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales.
Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

2.2.5 La capa de sesión

La capa de sesión es la que establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos (lleva el control de quien va a transmitir). Además de regular la sesión, esta capa ofrece disposiciones para una eficiente transferencia de datos (evita que dos partes intenten la misma operación al mismo tiempo), clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

2.2.6 La capa de presentación

La capa de presentación es la que se encarga de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

"*Para hacer posible la comunicación entre computadoras con distintas representaciones internas de datos, podemos definir de una manera abstracta las estructuras de datos que se van a intercambiar, junto con una codificación estándar que se use "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de mayor nivel (por ejemplo, registros bancarios)."* (Tanenbaum & Wetherall, 2012).

2.2.7 La capa de aplicación

La capa de aplicación es la capa más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI.

Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

"Contiene una gran variedad de protocolos que los usuarios necesitan con frecuencia, un protocolo de aplicación muy utilizado es ***HTTP*** *(Hyper Text Transfer Protocol) o Protocolo de Transferencia de Hipertexto, el cual forma la base para la* ***WWW*** *(World Wide Web). Cuando un navegador desea una página web, envía el nombre de la página que quiere al servidor que la hospeda mediante el uso de HTTP. Después el servidor envía la página de vuelta. Hay otros protocolos de aplicación que se utilizan para transferir archivos, enviar y recibir correo electrónico y noticias."* (Tanenbaum & Wetherall, 2012).

2.3 Modelo de referencia TCP/IP

El modelo **TCP/IP** es un modelo de descripción de protocolos de red desarrollado en el año de 1974 por Vinton Cerf y Robert E. Kahn. EL modelo TCP/IP se denomina a veces como Internet Model, Modelo DoD (Departament of the Defense) Departamento de Defensa de los Estados Unidos. Fue implementado por primera vez en ARPANET y posteriormente aplicado a lo que hoy se conoce como Internet. Ver ilustración 4

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

TCP/IP tiene cuatro capas de abstracción, esta arquitectura de capas a menudo es comparada con el Modelo OSI de siete capas.

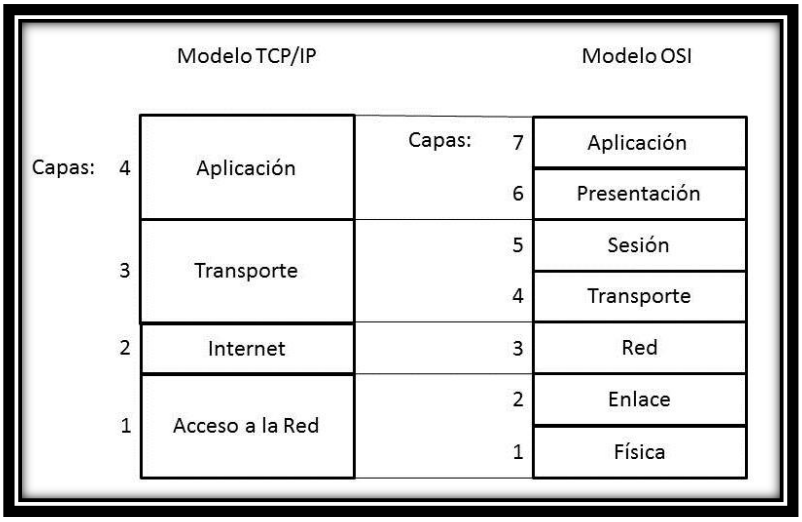

Ilustración 4 Modelo de referencia TCP/IP

2.3.1 La capa de acceso a red

La capa de acceso a la red es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red. Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local tales como cable coaxial, fibra óptica, par físico conectada mediante línea telefónica u otro tipo de conexión a una red.

2.3.2 La capa de internet

La capa de Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido.

Para el caso de los datagramas direccionados hacia la máquina local, el software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete.

En esta capa operan varios protocolos los cuales son; **IP** (Protocolo de Internet), **ICMP** (Protocolo de Internet de Control de Mensajes), **ARP** (Protocolo de Resolución de Dirección), **RARP** (Protocolo de Resolución de Dirección de Retorno) y **IGMP** (Protocolo de Administración de Grupos de Internet). De estos los primeros 3 son los más importantes de esta capa.

2.3.3 La capa de transporte

La función básica de la capa de transporte es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo, además, todo esto se debe hacer de manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. Simplemente especifican la manera de asegurar una transferencia confiable.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son **TCP** (Protocolo de Control de Transmisión), un protocolo orientado a conexión que brinda detección de errores **UDP** (Protocolo de Datagramas de Usuario), un protocolo no orientado a conexión en el que la detección de errores es obsoleta.

2.3.4 La capa de aplicación

La capa de aplicación se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores.

Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.
Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo.

La capa de aplicación soporta los protocolos de direccionamiento y la administración de red. Además tiene protocolos para transferencia de archivos, correo electrónico y conexión remota.

"Esta capa contiene todos los protocolos de alto nivel. En los primeros protocolos están el de terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP). A través de los años se han agregado muchos otros protocolos. El sistema de nombres de dominio (DNS) para resolución de nombres de Host a sus direcciones; HTTP, el tiempo para recuperar páginas de la World Wide Web; y RTP, el protocolo para transmitir medios en tiempo real, como voz o películas." (Tanenbaum & Wetherall, 2012).

2.4 Estándar IEEE 802

2.4.1 IEEE 802

Es un estudio de estándares elaborado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que actúa sobre Redes de ordenadores. De igual forma se refiere a los estándares que proponen, algunos de los cuales son muy conocidos tales como Ethernet (IEEE 802.3), o Wi-Fi (IEEE 802.11). Incluso hoy en día están intentando estandarizar Bluetooth en el 802.15 (IEEE 802.15).

Se centra en definir los niveles más bajos (según el modelo de referencia OSI o sobre cualquier otro modelo). Concretamente subdivide el segundo nivel, el de enlace, en dos subniveles: El de Enlace Lógico (LLC), recogido en 802.2, y el de Control de Acceso al Medio (MAC), subcapa de la capa de Enlace Lógico. El resto de los estándares actúan tanto en el Nivel Físico, como en el subnivel de Control de Acceso al Medio.

En febrero de 1980 se formó en el IEEE un comité de redes locales con la intención de estandarizar un sistema de 1 o 2 Mbps que básicamente era Ethernet (el de la época). Le tocó el número 802. Dividieron el nivel de enlace en dos subniveles: el de enlace lógico, encargado de la lógica de re-envíos, control de flujo y comprobación de errores, y el subnivel de acceso al medio, encargado de arbitrar los conflictos de acceso simultáneo a la red por parte de las estaciones.

Para finales del año 1980 ya se había ampliado el estándar para incluir el Token Ring (Red en anillo con paso de testigo) de IBM y un año después, y por presiones de grupos industriales, se incluyó Token Bus (Red en bus con paso de testigo), que incluía opciones de tiempo real y redundancia, y que se suponía idóneo para ambientes de fábrica.

Conforme avanzaba la tecnología, se fueron ampliando los campos de trabajo, se incluyeron redes de área metropolitana (alguna decena de kilómetros), personal (unos pocos metros) y regional (algún centenar de kilómetros), se incluyeron redes inalámbricas (WLAN), métodos de seguridad, comodidad, etc.

En este capítulo se explicará de manera general el funcionamiento del estándar IEEE 802.11. Cabe mencionar que no es la única que existe, esta familia de estándares tiene miembros diversos con diferencias tecnológicas y diferentes adaptaciones. Ver Tabla 1

"De las siete capas del modelo OSI, anteriormente ya mencionadas, El estándar IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas: la capa física y de enlace. En estas capas se define las técnicas de acceso, las cuales su funcionamiento es que cada terminal puede hacer uso del medio de comunicación común. Las primeras técnicas de acceso que definió el IEEE se pensaron para las redes de cable." (Gómez, 2011).

Nombre	Descripción	Nota
IEEE 802.1	Normalización de interface	
802.1D	Spanning Tree Protocol	
802.1Q	Virtual Local Area Networks (VLAN)	
802.1aq	Shortest Path Bridging (SPB)	
IEEE 802.2	Control de enlace lógico	Inactivo
IEEE 802.3	CSMA/CD (Ethernet)	
IEEE 802.4	Token bus	Disuelto
IEEE 802.5	Token ring	Inactivo
IEEE 802.6	Metropolitan Area Network (MAN)	Disuelto
IEEE 802.7	Grupo asesor en banda ancha	Disuelto
IEEE 802.8	Grupo asesor en fibras ópticas	Disuelto
IEEE 802.9	Servicios integrados de red de Área Local	Disuelto
IEEE 802.10	Seguridad	Disuelto
IEEE 802.11	Redes inalámbricas WLAN (Wi-Fi)	
IEEE 802.12	Prioridad por demanda	Disuelto
IEEE 802.13	Se ha evitado su uso por superstición	Sin uso
IEEE 802.14	Modems de cable	Disuelto
IEEE 802.15	WPAN (Bluetooth)	
IEEE 802.16	Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)	
IEEE 802.17	Anillo de paquete elástico	
IEEE 802.18	Grupo de Asesoría Técnica sobre Normativas de Radio	En desarrollo hoy en día
IEEE 802.19	Grupo de Asesoría Técnica de Coexistencia	
IEEE 802.20	Mobile Broadman Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Networks	

Tabla 1 Estándar 802

Esto llevo a una evolución de los estándares de IEEE para asegurar el correcto funcionamiento y que puedan trabajar sin ningún problema.

"En 1997 el IEEE añadió un nuevo miembro a su familia de 802 que se ocupa de definir las redes de área local inalámbricas. Este nuevo miembro es el 802.11.

La primera norma de 802.11 utilizaba infrarrojos como medio de transmisión y nunca tuvo una buena aceptación en el mercado. Posteriormente salieron otras dos nuevas normas de 802.11 basadas en el uso de radiofrecuencia en la banda 2,4 GHz. Ambas se diferencian en el método de transmisión de radio utilizado. Una utiliza el sistema FHSS (Frequency Hopping Spread Spectrum) o Difusión por Salto de Frecuencia, y la otra usa el sistema DSSS (Direct Sequence Spread Spectrum) o Difusión por Secuencia Directa." (Gómez, 2011).

No fue hasta 1999 en que aparecieron los primeros semiconductores de tecnología de radio de 2,4 GHz, esto a su vez dio paso para que la familia 802.11 se fortaleciera y con ello aparecen nuevas versiones del estándar 802.11. Ver Tabla 2

A continuación se mencionan algunas de ellas:

- **IEEE 802.11a** La revisión 802.11a fue aprobada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz, con una velocidad máxima de 54 Mbit/s, tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto

- **IEEE 802.11b** La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz.

- **IEEE 802.11g** En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a.

  Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados. Existe una variante llamada 802.11g+ capaz de alcanzar los 108 Mbps de tasa de transferencia, generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

- **IEEE 802.11n** En enero de 2004, se dio a conocer el IEEE 802.11n. La velocidad real de transmisión máxima es de 600 Mbps, aunque su velocidad promedio es de 300 Mbps. Este estándar se viene implantando desde 2008.

  A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Debido a esto, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.

ESTANDAR	AÑO	DESCRIPCION
802.11	1997	Especificaciones de la capa física y MAC, de las redes de área local inalámbricas (infrarrojo y radio 2,4 GHz).
802.11ª	1999	Especificaciones para redes inalámbricas de alta velocidad (54 Mbps) en la banda de 5 GHz.
802.11b	1999	Especificaciones de la capa física y MAC de las redes de área local inalámbricas de rango de velocidad de 5,5 a 11 Mbps /radio 2,4 GHz).
802.11c	1998	Define las características que necesitan los puntos de acceso para actuar como puentes (bridges).
802.11d	2001	Adaptación a los requerimientos regionales (modo mundial)
802.11e	2005	Calidad de servicio para aplicaciones en tiempo real (voz, video, etc.).
802.11f	2000	Interoperatividad entre puntos de acceso de distintos fabricantes (Interaccess Point Protocol, IAPP) para permitir la itinerancia (Roaming).
802.11g	2003	Especificaciones para redes inalámbricas de alta velocidad (54 Mbps) en la banda de 2,4 GHz.
802.11h	2003	Mejoras en la gestión del espectro (selección dinámica de canal y control de potencia de transmisión).
802.11i	2004	Mejoras para seguridad y autentificación.
802.11j	2004	802.11a con canales adicionales por encima de 4,9 GHz (802.11a en Japón).
802.11k	2002	Intercambio de información de capacidad entre clientes y puntos de acceso.
802.11m	2003	Estándar propuesto para el mantenimiento de redes inalámbricas.
802.11n	2004	Nueva generación para redes inalámbricas de alta velocidad (hasta 540 Mbps teóricos).Existen propuestas para 2,4 y 5 GHz.
80211p	2008	Acceso inalámbrico para el entorno de vínculos (coches, ambulancias, etc.).
802.11r	2008	Permite establecer protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él en menos de 50 milisegundos.
802.11v	2011	Aun en pruebas. Permitirá la configuración remota de los dispositivos cliente, incluye mecanismos de ahorro de energía, mejor posicionamiento, temporización y coexistencia.
802.11w	2009	Aún en pruebas. Permitirá aumentar la seguridad de los protocolos de autenticación y codificación.

Tabla 2 Estándares IEEE 802.11

Una de las claves del éxito comercial ha sido la buena interoperabilidad existente entre equipos de diferentes fabricantes, labor que ha llevado a cabo la Wi-Fi Alliance. Este organismo, con cerca de 200 empresas entre sus miembros y 800 productos certificados al día de hoy ha fomentado la tecnología y garantizando su genérico buen uso.

2.5 Topologías de red

La topología de red se define como una familia de comunicación usada por las computadoras que conforman una red para intercambiar datos, esto es en la forma en que está diseñada la red, sea en el plano físico o lógico.

El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos refiramos. Es la distribución geométrica de las computadoras conectadas.

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en cómo se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación.

2.5.1 Red en Bus

Una topología de bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos en la red. Ver ilustración 5

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente. La ruptura del cable hace que los hosts queden desconectados.

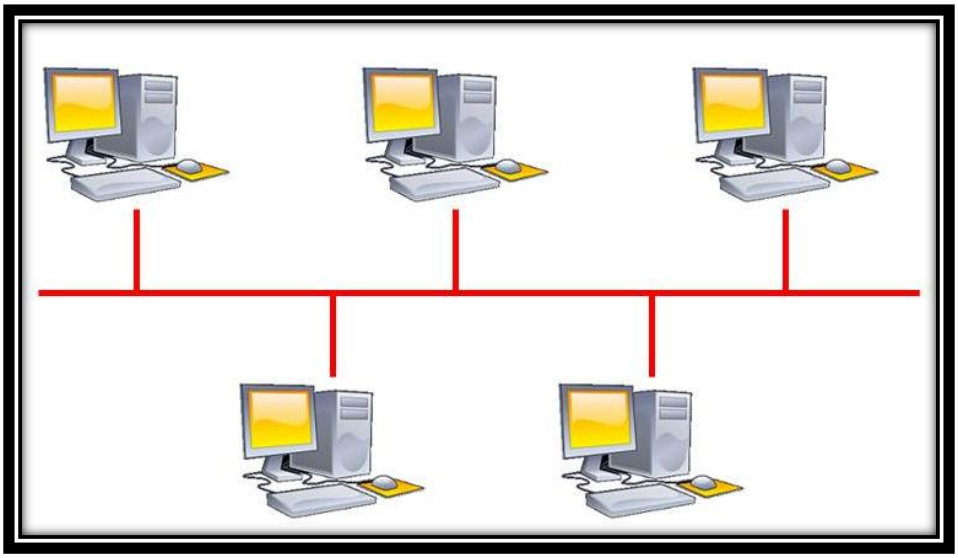

Ilustración 5 Topología en bus

Los extremos del cable se terminan con una resistencia de acople denominada terminador, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus por medio de un acople de impedancias.

Si se produce una rotura en cualquier parte del cable o si un extremo no está terminado, la señal balanceará hacia adelante y hacia atrás a través de la red y la comunicación se detendrá.

El número de equipos presentes en un bus también afecta al rendimiento de la red. Cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus, y en consecuencia, la red irá más lenta.

Además, debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho ruido. Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente. Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.

Ventajas:

Facilidad de implementación y crecimiento.
Económica.
Simplicidad en la arquitectura

Desventajas:

Longitudes de canal limitadas.Un problema en el canal usualmente degrada toda la red.
El desempeño se disminuye a medida que la red crece.
El canal requiere ser correctamente cerrado (caminos cerrados).Altas pérdidas en la transmisión debido a colisiones entre mensajes.

2.5.2 Red en Anillo

En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor. Ver ilustración 6

En este tipo de red la comunicación se da por el paso de un Token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

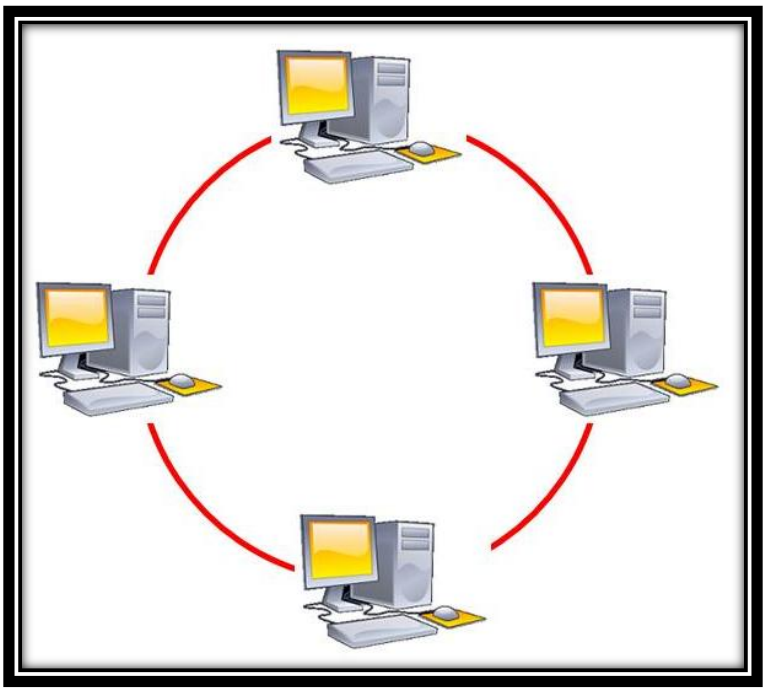

Ilustración 6 Topología en anillo

Cabe mencionar que si algún nodo de la red deja de funcionar, la comunicación en todo el anillo se pierde.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que si uno de los anillos falla, los datos pueden transmitirse por el otro.

Ventajas:

Simplicidad de arquitectura. Facilidad de implementación y crecimiento.

Desventajas:

Longitudes de canal limitadas.
El canal usualmente degradará a medida que la red crece.

2.5.3 Red en Estrella

En una topología en estrella, los segmentos de cable de cada equipo en la red están conectados a un componente centralizado, o concentrador. Un concentrador es un dispositivo que conecta varios equipos juntos. Ver ilustración 7

Dado su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

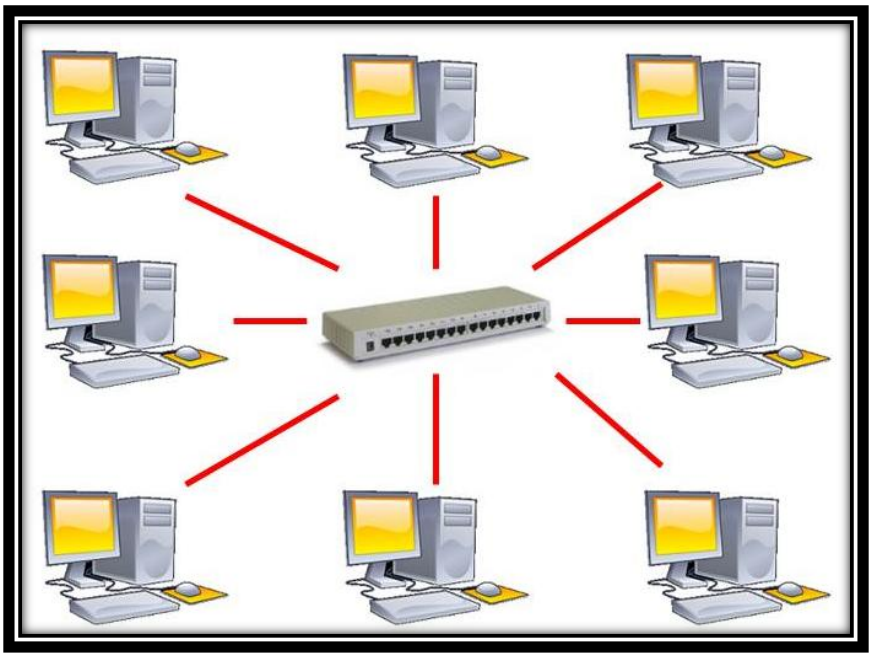

Ilustración 7 Topología en estrella

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (Router), un conmutador (Switch) o un concentrador (Hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

Ventajas:

Tiene dos medios para prevenir problemas.
Permite que todos los nodos se comuniquen entre sí de manera conveniente.

Desventajas:

Si el nodo central falla, toda la red se desconecta.
Es costosa, ya que requiere más cable que la topología bus.
El cable viaja por separado del Hub a cada computadora.

2.5.4 Red en Malla

En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta. Ver ilustración 8

De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

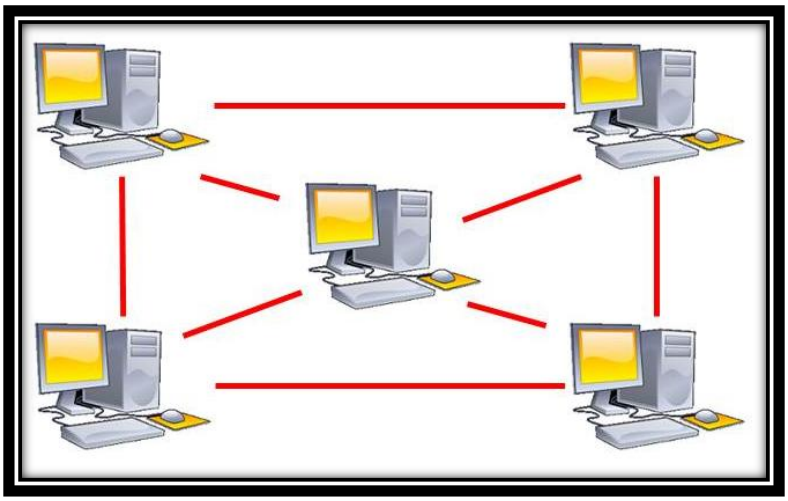

Ilustración 8 Topología en malla

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que los elementos de la red (nodo) están conectados todos con todos, mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red de modo que, si falla un cable, otro se hará cargo del tráfico.

Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).

Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Ventajas:

El uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos.
Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes.
Si un enlace falla, no inhabilita todo el sistema.

Desventajas:

Su principal desventaja es que funciona con pocos ordenadores debido a que están conectados físicamente y si la cantidad de ordenadores es muy grande las conexiones serían abrumadoras es por ello que solo se utiliza en redes pequeñas.
Es más costosa que las demás topologías debido a que utilizan mayor cantidad de cableado.
Debido a que su instalación, configuración y mantenimiento son muy difíciles ya que los ordenadores deben estar conectados entre sí que, a su vez, ocupa demasiado espacio.

2.5.5 Red en Árbol

La topología en árbol es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red.

Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central. Ver ilustración 9

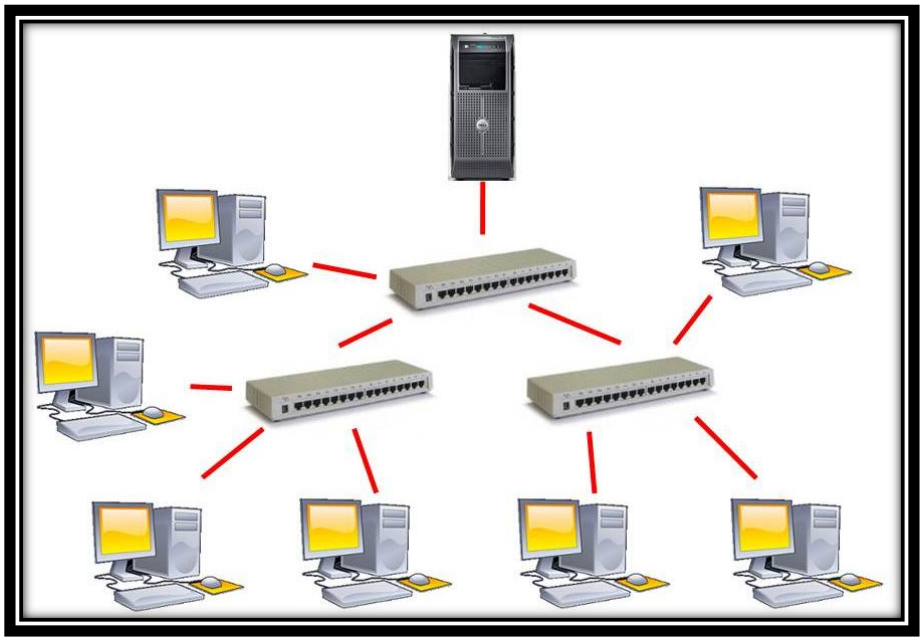

Ilustración 9 Topología en árbol

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

Ventajas:

El Hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.
Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
Permite priorizar y aislar las comunicaciones de distintas computadoras.
Cableado punto a punto para segmentos individuales.
Soportado por multitud de vendedores de software y de hardware.

Desventajas:

Se requiere mucho cable.
La medida de cada segmento viene determinada por el tipo de cable utilizado.
Si se viene abajo el segmento principal todo el segmento se viene abajo con él.
Es más difícil su configuración.
No tiene sentido único.

2.6 Clasificación de las Redes

Las redes se pueden clasificar de distintas formas, puede hacerse teniendo en cuenta el espacio físico por el que se encuentran distribuidas, de esta forma las clasificaremos por su cobertura.

2.6.1 Por alcance

PAN (Personal Área Network), Red de Área Personal

Se establece que las redes de área personal son una configuración básica llamada así mismo personal la cual está integrada por los dispositivos que están situados en el entorno personal y local del usuario, ya sea en la casa, trabajo, carro, parque, centro comercial, etc. Esta configuración le permite al usuario establecer una comunicación con estos dispositivos a la hora que sea de manera rápida y eficaz. Ver ilustración 10

Algunas empresas se pusieron de acuerdo para diseñar una red inalámbrica de corto alcance conocida como Bluetooth para conectar estos componentes sin necesidad de cables. Las redes Bluetooth utilizan el paradigma maestro – esclavo, la unidad de sistema (PC), por lo general es el maestro, que trata con el ratón, teclado, impresoras, teléfonos celulares, etc., como sus esclavos. El maestro les indica que direcciones usar, cuando pueden transmitir información y por cuanto tiempo pueden transmitir, que frecuencias usar, entre otras cosas.

Ilustración 10 PAN (Personal Area Network)

LAN (Local Área Network), Red de Área Local

Una red LAN conecta varios dispositivos de red en una área de corta distancia (decenas de metros) delimitadas únicamente por la distancia de propagación del medio de transmisión como coaxial (hasta 500 metros), par trenzado (hasta 90 metros) o fibra óptica (decenas de metros), espectro disperso o infrarrojo (decenas de metros). Ver ilustración 11

En estos sistemas, cada computadora tiene un módem y una antena que utiliza para comunicarse con otras computadoras. En la mayoría de los casos cada computadora se comunica con un dispositivo en el techo a este dispositivo se le denomina AP (Access Point) o Punto de Acceso, el cual transmite paquetes entre las computadoras inalámbricas y también entre estas e Internet.

Una LAN podría estar delimitada también por el espacio en un edificio, un salón, una oficina, hogar…pero a su vez podría haber varias LAN en estos mismos espacios. Se caracterizan por: tamaño restringido, tecnología de transmisión, alta velocidad y topología.

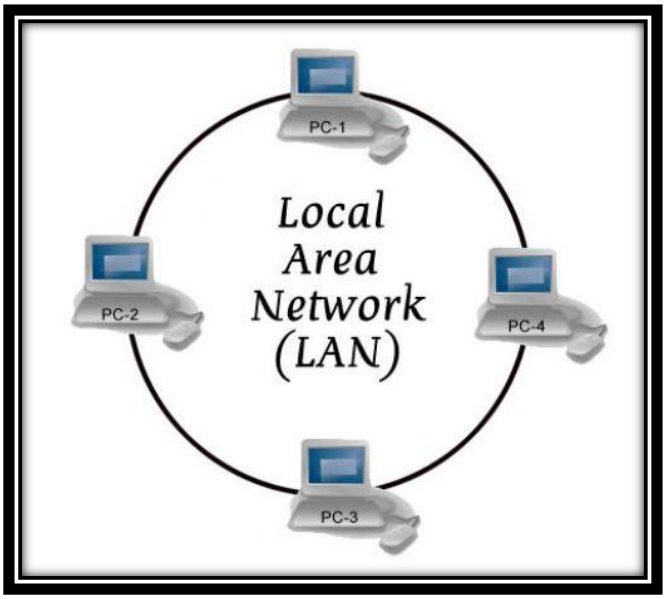

Ilustración 11 LAN (Local Área Network)

Este tipo de redes maneja un estándar llamado IEEE 802.11, mejor conocido como Wi-Fi que operan a una velocidad de 11 hasta cientos de Mbps, el cual tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos. En redes basadas en IP, se puede concebir una LAN como una subred, pero esto no es necesariamente cierto en la práctica.

Las LAN comúnmente utilizan las tecnologías Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) para conectividad, así como otros protocolos tales como Appletalk, Banyan Vines, DECnet, IPX, etc. CAN: Campus Área Network, Red de Área Campus.

En resumen, las redes LAN domésticas ofrecen muchas oportunidades y retos. La mayoría de estos retos se relacionan con la necesidad de que las redes sean más fáciles de manejar, confiables y seguras (en especial de manos de usuarios inexpertos), así como de un bajo costo.

CAN (Campus Área Network), Red de área de campus

Es una colección de LAN dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilómetros. Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso. No utiliza medios públicos. Ver ilustración 12

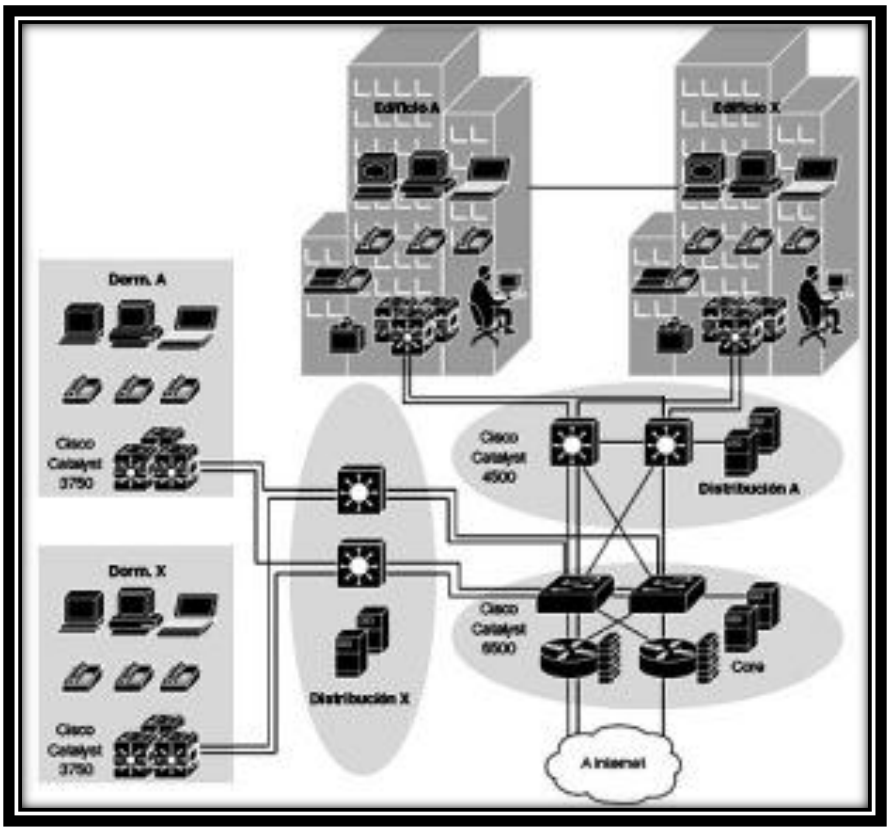

Ilustración 12 CAN (Campus Área Network)

MAN (Metropolitana Área Network), Red de Área Metropolitana

Una MAN es una colección de LAN o CAN dispersas en una ciudad (decenas de kilómetros), da cobertura en un área geográfica más extensa que un campus, pero aun así, limitada. Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL (Digital Subscriber Line), WDM (Wavelenght Division Modulation), ISDN, E1/T1, PPP, etc. Para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

Una MAN puede soportar tanto voz como datos, tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño. Ver ilustración 13

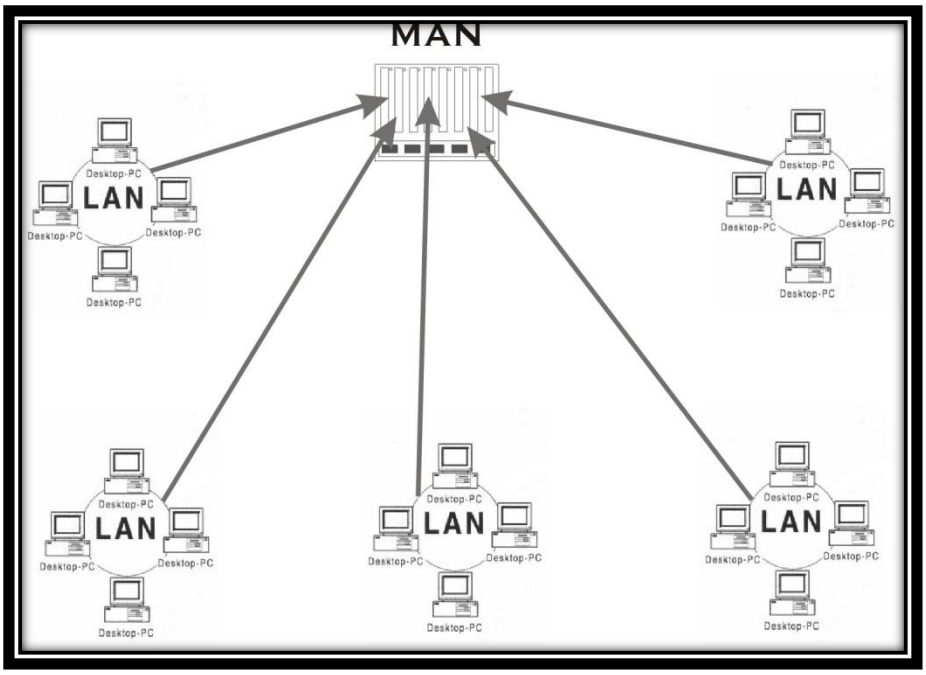

Ilustración 13 MAN (Metropolitana Área Network)

WAN (Wide Área Network), Red de Área Amplia

Una WAN es una colección de LAN dispersadas geográficamente cientos de kilómetros una de otra, un ejemplo de ellos es que abarcan un país o un continente completo. Un dispositivo de red llamado enrutador es capaz de conectar LAN a una WAN.

Las WAN utilizan comúnmente tecnologías ATM (Asynchronous Transfer Mode), Frame Relay, X.25, E1/T1, GSM, TDMA, CDMA, xDSL, PPP, etc. para conectividad a través de medios de comunicación tales como fibra óptica, microondas, celular y vía satélite.

Otros tipos de redes WAN utilizan mucho las tecnologías inalámbricas. En los sistemas de satélite, cada computadora en la Tierra tiene una antena a través de la cual es posible enviar y recibir datos de un satélite en órbita. Ver ilustración 14

Todas las computadoras pueden escuchar la salida proveniente del satélite y, en algunos casos, también pueden escuchar las transmisiones que envían sus computadoras vecinas hacia el satélite. Las rede de satélite son de difusión por naturaleza y son más útiles cuando es importante contar con la propiedad de difusión.

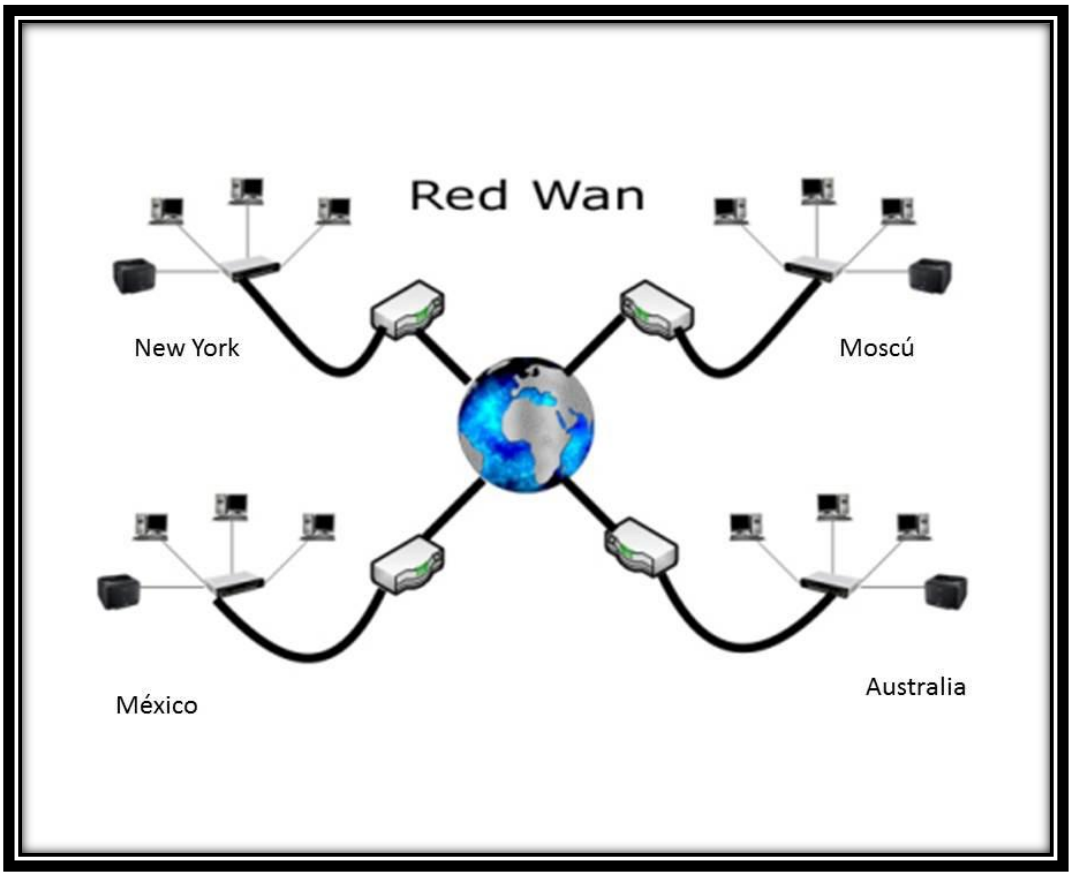

Ilustración 14 WAN (Wide Área Network)

La red de telefonía celular es otro ejemplo de una WAN que utiliza tecnología inalámbrica. Este sistema ya pasó por tres generaciones y hay una cuarta por venir. La primera generación fue análoga y sólo para voz. La segunda fue digital y sólo para voz.

La tercera generación es digital y se puede transmitir tanto datos como voz. Cada estación base en un sistema celular cubre una distancia mucho mayor que una LAN inalámbrica, en donde el rango se mide en kilómetros en vez de decenas de metros.

Las estaciones base se conectan entre sí mediante una red troncal que por lo general es alámbrica. Las velocidades de datos de las redes celulares se encuentran comúnmente en el orden de 1 Mbps, un valor mucho menor al de una LAN inalámbrica que puede estar en el orden de hasta 100 Mbps.

2.6.2 Por tipo de conexión

Medios guiados

El cable coaxial: se utiliza para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.

El cable de par trenzado: es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.

La fibra óptica: es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Medios no guiados

Red por radio: Es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red. Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores.

Los dispositivos inalámbricos que permiten la constitución de estas redes utilizan diversos protocolos como el Wi-Fi: El estándar IEEE 802.11. El cual es para las redes inalámbricas, lo que Ethernet para las redes de área local (LAN) cableadas. Además del protocolo 802.11 del IEEE existen otros estándares como el HomeRF, Bluetooth y ZigBee.

Red por infrarrojos: Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación por ello es escasa su utilización a gran escala. Esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos (Bluetooth, Wireless, etcétera).

Se utiliza principalmente para realizar intercambio de datos entre dispositivos móviles, como PDA's o móviles, ya que el rango de velocidad y el tamaño de los datos a enviar/recibir es pequeño.

Red por microondas: Es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b. Muchas empresas que se dedican a ofrecer servicios de Internet, lo hacen a través de las microondas, logrando velocidades de transmisión y recepción de datos de 2.048 Mbps, o múltiplos.

El servicio utiliza una antena que se coloca en un área despejada sin obstáculos de edificios, árboles u otras cosas que pudieran entorpecer una buena recepción en el edificio o la casa del receptor y se coloca un módem que interconecta la antena con la computadora. La comunicación entre el módem y la computadora se realiza a través de una tarjeta de red, que deberá estar instalada en la computadora.

2.6.3 Por grado de autentificación

Red pública: Abarca todo el mundo. Una red WAN, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 Km., dando el servicio a un país o un continente.

Un ejemplo de este tipo de redes sería Red IRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

Red privada: Alguna gente. Una red de LAN, es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros.

Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

2.6.4 Por relación funcional

Cliente-servidor: es una arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

Peer-to-peer: es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

2.6.5 Por grado de difusión

Intranet: es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada, esto es, que no comparte sus recursos o su información con redes ilegítimas.

Internet: es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

2.7 Red inalámbrica

Una red inalámbrica es aquella que permite conectar diversos nodos sin utilizar una conexión física, sino estableciendo la comunicación mediante ondas electromagnéticas. La transmisión y la recepción de los datos requieren de dispositivos que actúan como puertos. Las redes inalámbricas permiten establecer vínculos entre computadoras y otros equipos informáticos sin necesidad de instalar un cableado, lo que supone una mayor comodidad y un ahorro de dinero.

Como punto negativo, este tipo de redes suele contar con una seguridad menor ya que, si no se cuenta con una protección eficiente, el ingreso de intrusos es muy probable.

A continuación se dan a conocer algunos beneficios de la tecnología de red inalámbrica así como una breve guía sobre los ahorros de costos y otros, junto con información acerca de las soluciones de red inalámbrica de Cisco para empresas en crecimiento, las cuales son:

- **Económica.** Como elimina o reduce los gastos de cableado, cuesta menos instalar, operar y ampliar una red inalámbrica en comparación con una red cableada.

- **Cómodo acceso.** Obtenga acceso a los recursos de la red desde cualquier lugar dentro del área de cobertura de la red inalámbrica, como salas de conferencias, o desde cualquier punto de acceso inalámbrico público.

- **Fácil configuración y expansión.** Con una red inalámbrica no es necesario instalar cables para conectar computadoras, impresoras y otros dispositivos a Internet. También es sencillo agregar nuevos usuarios de computadoras a la red.

- **Segura.** Los continuos avances en normas y protocolos han logrado que las redes inalámbricas sean, en muchos casos, tan seguras como las redes cableadas. Una red inalámbrica ofrece sólidas funciones de seguridad tales como cifrado de datos, para proteger a la información que viaja por la red; autenticación de usuarios, que identifica a las computadoras que intentan acceder a la red; y acceso seguro para visitantes y usuarios temporales.

2.7.1 Red Wi-Fi

Wi-Fi (Wireless Fidelity) Se le denomina a una red que cumple los estándares 802.11 relacionados a redes inalámbricas de área local. Las redes Wi-Fi emplean ondas de radio para conectar dispositivos, como por ejemplo ordenadores portátiles a Internet, a las aplicaciones y a la red de su negocio.

La señal de un router o de un punto de acceso Wi-Fi tiene un alcance aproximado de unos 90 metros. Era una creencia extendida que las redes por cable eran más rápidas y seguras que las Wi-Fi. Sin embargo, las continuas mejoras de los estándares y tecnologías Wi-Fi han eliminado en gran medida estas diferencias.

La red Wi-Fi habitualmente se encuentra en lugares públicos, tales como cafés, hoteles y salas de espera de aeropuertos, y también muchas empresas poseen redes Wi-Fi en todos los edificios de sus oficinas o en sus campus, para su uso por parte de empleados e invitados. De igual forma y en lo que nos enfocaremos es en su uso para hogares.

Muchos routers funcionan como puntos de acceso W-iFi. Conectan múltiples ordenadores (e impresoras con acceso inalámbrico) a una única red Wi-Fi y a Internet. Este tipo de redes puede extenderse por un área a través de la colocación de puntos de acceso W-iFi adicionales en distintos emplazamientos. Los puntos de acceso amplían el alcance y potencia de la señal.

Muchos ordenadores portátiles poseen funciones de red Wi-Fi integradas. Si su ordenador no dispone de ellas, necesitará una tarjeta adaptadora de red inalámbrica, que suele ser económica y de fácil instalación.

2.7.2 Ventajas y desventajas de Wi-Fi

Ventajas

- No existen cables físicos (no hay cables que se enreden).
- Poder conectarse desde cualquier lugar que se encuentre dentro del rango de cobertura de la red.
- Su instalación es rápida y rentable.
- Al no haber cables de por medio, este tipo de redes son más baratas que las cableadas.
- Elección de entre varias señales libres o con seguridad.
- Al ser redes inalámbricas, la comodidad que ofrecen es superior a las cableadas.
- De igual forma la movilidad en este tipo de redes, lo que nos indica que podemos seguir conectados aun estando en movimiento.

Desventajas

- La principal desventaja de este tipo de redes es la seguridad (más adelante hablaremos de ello).
- La señal puede bloquearse o presentar interferencias.
- Todavía no hay estudios certeros sobre la peligrosidad (o no) de las radiaciones utilizadas en las redes inalámbricas.
- La velocidad que alcanzan es baja en comparación con la de un cable de red.
- Distancia limitada para la recepción de la señal, saliendo del rango de cobertura de red, se pierde toda conexión.

2.7.3 Sistema de red WEP

Tiempo después de que apareciera la tecnología inalámbrica Wi-Fi. El único sistema de seguridad que incluía era el cifrado **WEP** (Wired Equivalency Protocol) o Protocolo de Equivalencia con la Red. Introducido como parte de la original de 802.11 ratificado en septiembre de 1999, su intención es la de garantizar la confidencialidad de datos comparable a la de una red cableada tradicional, WEP es ampliamente utilizado y es a menudo la opción de seguridad presentado por primera vez a los usuarios por la configuración del router.

El Estándar de 64-bit WEP utiliza una clave de 40 bits (también conocido como WEP-40), que se concatena con un vector de inicialización de 24 bits (IV) para formar la clave del tráfico RC4. Una clave de 128-bit WEP es casi siempre introducidos por los usuarios como una cadena de 26 caracteres hexadecimales (base 16) caracteres (0-9 y A-Z). Cada personaje representa cuatro bits de la clave. 26 dígitos de cuatro bits cada uno da 104 bits, la adición de la IV de 24 bits produce la final de 128 bits clave WEP.

Un sistema de 256-bit WEP está disponible en algunos fabricantes, y como con el sistema de clave de 128 bits, 24 bits de que es para el IV, dejando 232 bits reales para su protección. Estos 232 bits se suele introducir como 58 caracteres hexadecimales. (58 x 4 = 232 bits) + 24 bits IV = 256 bits clave WEP.

"Para garantizar la integridad, el texto original se envía junto con lo que se conoce como ICV (Integrity Check Value) o Valor de Comprobación de Integridad. Se trata de 32 bits de comparación de integridad que se calcula con otro algoritmo llamado CRC-32 (Cyclic Redundancy Check) o Código de Redundancia Cíclica de 32 bits." (Gómez, 2011). Ver ilustración 15

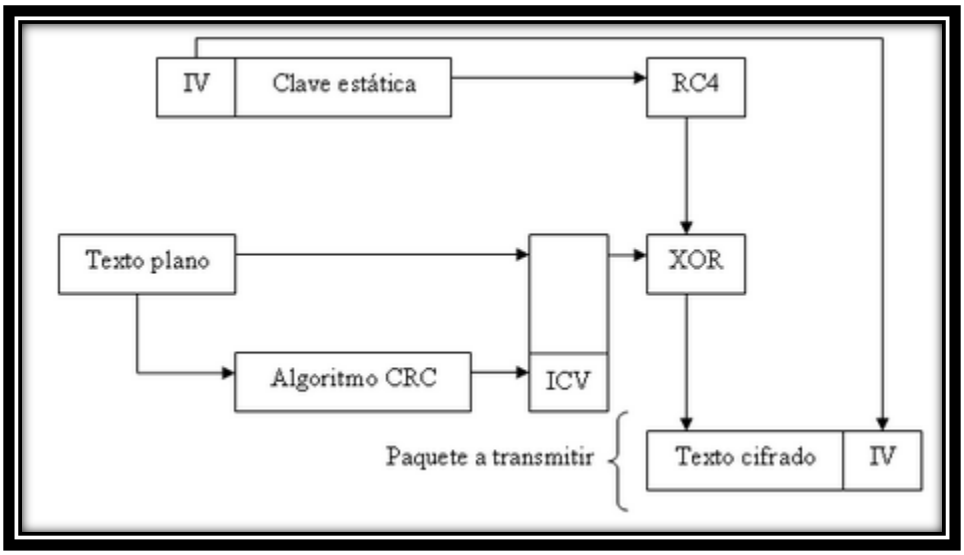

Ilustración 15 Proceso de cifrado WEP

Desde entonces, se ha aceptado que WEP proporciona un nivel de seguridad aceptable sólo para usuarios domésticos y aplicaciones no críticas. Sin embargo, incluso eso se desvaneció con la aparición de los ataques KoreK en 2004 (ataques generalizados FMS, que incluían optimizaciones de h1kari), y el ataque inductivo invertido Arbaugh, permitiendo que paquetes arbitrarios fueran des encriptados sin necesidad de conocer la clave utilizando la inyección de paquetes.

Las herramientas de cracking, como Backtrack 5, ponen en práctica estos ataques y pueden extraer una clave WEP de 128-bits en menos de 10 minutos (o algo más, dependiendo del punto de acceso y la tarjeta Wireless específicos).

La incorporación de la inyección de paquetes mejoró sustancialmente los tiempos de crackeo de WEP, requiriendo tan sólo miles, en lugar de millones, de paquetes con suficientes IVs únicos – alrededor de 150,000 para una clave WEP de 64-bits y 500,000 para una clave de 128-bits. Con la inyección de paquetes, el obtener los datos necesarios era apenas una tarea de minutos. En la actualidad, WEP está definitivamente muerto.

"La WECA (la asociación de fabricantes de productos y servicios inalámbricos que certifica los equipos) siempre ha respondido a estos informes diciendo que los ataques siempre utilizan sistemas muy sofisticados (aunque más adelante veremos lo contrario). En cualquier caso, tanto WECA como IEEE han trabajado para ofrecer una alternativa a WEP que ofrezca mayores niveles de seguridad: Los resultados han sido WPA y IEEE 802.11i." (Gómez, 2011).

2.7.4 Sistema de red WPA

En 2003 se propone el **WPA** (Wi-Fi Protected Access) o Acceso Protegido a Wi-Fi y luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 en 2004.

WPA: Publicado oficialmente por WECA a principios de 2003, el cual tiene la ventaja de ser compatible con el hardware existente con la recomendación de actualizar su firmware.

WPA2: Denominado estándar 802.11.i, publicado oficialmente por IEEE en junio de 2004, Aunque no es compatible con el hardware anterior, tiene la ventaja de ser más seguro y fiable. Este estándar también se conoce como RSN (Robust Security Network) o Red de Seguridad Robusta.

WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. Si no se usa un servidor de llaves, todas las estaciones de la red usan una **PSK** (Pre-Shared-Key) o llave previamente compartida, El modo PSK se conoce como WPA o WPA2-Personal. Cuando se emplea un servidor de llaves, al WPA2 se le conoce como WPA2-Corporativo o (WPA2-Enterprise). En WPA-Corporativo, se usa un servidor IEEE 802.1X para distribuir las llaves.

Una mejora notable en el WPA sobre el viejo WEP es la posibilidad de intercambiar llaves de manera dinámica mediante un **TKIP** (Temporal Key Integrity Protocol) o Protocolo de Integridad Temporal de Llaves.

La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i WPA2, el cual estaba por llegar. Para ello utiliza el protocolo **TKIP** y mecanismos 802.1x. La combinación de estos dos sistemas proporciona una encriptación dinámica y un proceso de autentificación mutuo. Así pues, WPA involucra dos aspectos: un sistema de encriptación mediante TKIP y un proceso de autentificación mediante 802.1x.

El proceso de encriptación es similar al realizado en WEP, pero con varias diferencias. Para empezar, si bien TKIP usa el algoritmo RC4 proporcionado por RSA Security para encriptar el cuerpo del frame así como el CRC antes de la transmisión, en este caso se utilizan IV de 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación.

Por otro lado y a diferencia de WEP, WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes lo que evita que la misma clave se utilice durante semanas, meses o incluso años, como pasaba con WEP.

WPA implementa lo que se conoce como **MIC** o (Message Integrity Code) o Código de Integridad del Mensaje. El MIC 8 bytes, un sistema de comprobación de la integridad de los mensajes, que se instala justo antes del ICV. Para el proceso de autentificación WPA y WPA2 usan una combinación de sistemas abiertos y 802.1x. El funcionamiento es igual al ya comentado en el apartado del 802.1x. Inicialmente el cliente se autentifica con el **AP** (Access Point) o Punto de Acceso, el cual le autoriza a enviarle paquetes.

"En definitiva, WPA ofrece soluciones para las principales deficiencias de WEP: ya que mejora el cifrado de datos mediante TKIP, utiliza claves dinámicas y permite la distribución automática de las claves así mismo proporciona una autentificación fuerte acorde al estándar de IEEE 802.1x.

En cuanto a WPA2 la principal diferencia con los sistemas de cifrado anteriores es que se utiliza el cifrado de bloques ***AES*** *(Advance Encryptio Syandar) o Estándar de Cifrado Avanzado. A diferencia de sus predecesores WEP y WPA quienes utilizaban el cifrado de flujo RC4."* (Gómez, 2011).

Capítulo 3

3.0 Testeo e Infiltración en redes Wi-Fi

Con el aumento significativo día con día de personas que utilizan redes inalámbricas, es más común el uso de estas en diferentes ámbitos desde el hogar hasta grandes empresas, debido a esto es más común los ataques por este tipo de redes. No se necesita ser un “hacker” para realizar este tipo de ataques, solo se necesita tener algunos conocimientos básico para lograrlo, esto quiere decir que cualquier persona experta o no en el tema de seguridad de redes inalámbricas puede acceder a una red solo en unos cuantos pasos y unos minutos que le llevará el proceso de infiltración.

Hoy en día hay diferentes programas y herramientas que hacen más fácil el testeo y la infiltración a redes inalámbricas con seguridad WEP y WPA principalmente.

La mayoría de este software es libre (se le dice software libre a la libertad de todos los usuarios que adquirieron el producto y, por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado, y redistribuido libremente de varias formas) y por lo tanto no tiene costo alguno para adquirirlo.

La mayoría de este software y/o herramientas trabajan sobre sistemas operativos de software libre, un ejemplo básico es GNU/Linux, aunque también existen programas que trabajan sobre las plataformas de Windows y Mac OS.

Algunos se pueden usar desde un LiveCD y otros simplemente se pueden hacer portátiles lo que nos ayuda a usarlo en cualquier momento y en cualquier lugar sin importar el sistema operativo que tengamos instalado en nuestra computadora.

3.1 Programas más usados para el testeo de señales

A continuación se dan a conocer algunas de las herramientas y software más usados que se ocupan principalmente para el testeo e infiltración de redes inalámbricas:

3.1.1 Beini

Es un sistema completo desarrollado para comprobar la seguridad de las redes wireless, basado en Tiny Core Linux. FeedingBottle, la GUI de aircrack-ng de Beini.

Beini es una mini distribution GNU/Linux que les va a permitir probar la seguridad de un punto de acceso Wifi. También, que está basada en Tiny Core Linux, y que es muy ligera pues con un peso de 47 Mb, el peso del archivo de descarga.

Sin embargo, Beini, tiene una particularidad. Tiene numerosas herramientas, entre las que podemos citar algunas: Aircrack-ng, Minidwep-gtk, Bib, etcétera.

3.1.2 Wifiway

Es una distribución de seguridad Wi-Fi basada en Linux From Scratch. Con Wifiway, podréis realizar auditorías en vuestras red inalámbricas Wi-Fi utilizando herramientas como Kismet, Aircrack, Airodump o Wireshark. La gran ventaja de la distribución Wifiway, radica en la integración de todas las herramientas necesarias a la hora de realizar ataques y análisis de redes inalámbricas Wi-Fi bajo GNU/Linux.

3.1.3 Wifislax

Es una distribución de seguridad informática orientada a la seguridad en redes Wi-Fi. Está disponible en formato Live CD, y a continuación se detallarán sus características, su ubicación de descarga, así como su disponibilidad en diversos soportes como USB, CD-Rom, etcétera.

3.1.4 Aircrack

Es un programa crackeador de claves WEP 802.11 y claves WPA-PSK que es capaz de recuperar las claves una vez que haya conseguido suficientes paquetes de datos. Implementa el ataque estándar FMS junto con algunas optimizaciones como los ataques Korek, así como todos los nuevos ataques PTW y como consecuencia obtiene un resultado de ataque mucho más rápido comparado con otras herramientas de crackeo WEP. De hecho, Aircrack-ng es un conjunto de herramientas para auditar redes Wi-Fi.

3.1.5 Wifi Auditor

Es un programa gratuito de código abierto (OPENSOURCE) que te permitirá realizar auditorías en tu red wifi para comprobar si la clave de nuestra red Wi-Fi que tenemos es segura evitando así posibles ataques de intrusos en nuestra red y mejorando la seguridad de la misma.

La aplicación descifra al instante muchas claves por defecto tipo WPA-PSK osea las que vienen de casa con el Router. Solamente funcionará cuando no se haya mejorado la seguridad de una red, es decir funcionará cuando no se hayan cambiado las claves que traen inicialmente los Routers.

Esto nos servirá para hacer auditorías Wi-Fi y comprobar si la clave que tiene nuestro Router es segura**.**

3.2 Criptografía

La criptografía es el arte o la ciencia de cifrar o descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología que engloba tanto a las técnicas de cifrado, es decir la criptografía como sus técnicas complementarias entre las cuales se incluye el criptoanálisis que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de claves.

A lo largo de la historia el ser humano ha desarrollado sistemas de seguridad que le permiten comprobar en una comunicación la identidad del interlocutor, asegurarse que solo obtendrá la información el destinatario solicitado y que además ésta no podrá ser modificada e incluso que ninguna de las 2 partes podrá negar el hecho de cuando fue enviado y recibido el mensaje. Ver ilustración 16

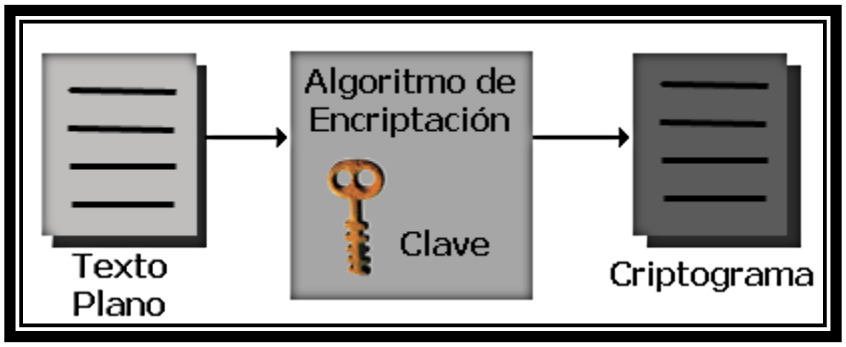

Ilustración 16 Ejemplo de encriptación

En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que contrasta con el documento de identidad.

Actualmente con el continuo crecimiento de Internet, cada vez se hacen mayor los números de mensajes que se están trasladando al mundo electrónico a través de correos electrónicos, mensajes privados, redes sociales, etcétera. Por lo cual necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el añadido de ofrecer garantías de seguridad aun sin presencia física.

Ante tales amenazas, la única solución consiste en proteger nuestros datos mediante el uso de técnicas criptográficas. Esto nos permitirá asegurar al menos dos elementos básicos de la Seguridad Informática, a saber la confidencialidad o secreto de la información y la integridad del mensaje, además de la autenticidad del emisor.

En la criptografía, la información original que debe protegerse se denomina texto en claro o texto plano, el cifrado es el proceso de convertir el texto plano en un galimatías ilegible denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (cifra) se basa en la existencia de una clave, información secreta que adapta el algoritmo de cifrado para cada uso distinto.

Las 2 técnicas más sencillas de cifrado en la criptografía clásica son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje, las letras, los símbolos o los dígitos) y la transposición (supone una reordenación de los mismos).

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utiliza los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios es lo que constituye en conjunto un criptosistema que es con lo que el usuario final trabaja e interactúa.

Existen 2 grandes grupos de cifrados, los algoritmos que solo utilizan una clave tanto en el proceso de cifrado como en el de descifrado y los que emplean una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifrados simétricos de clave simétrica o de clave privada y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifrados asimétricos de clave asimétrica o de clave pública y forman el núcleo de las técnicas de cifrado modernas. Ver ilustración 17

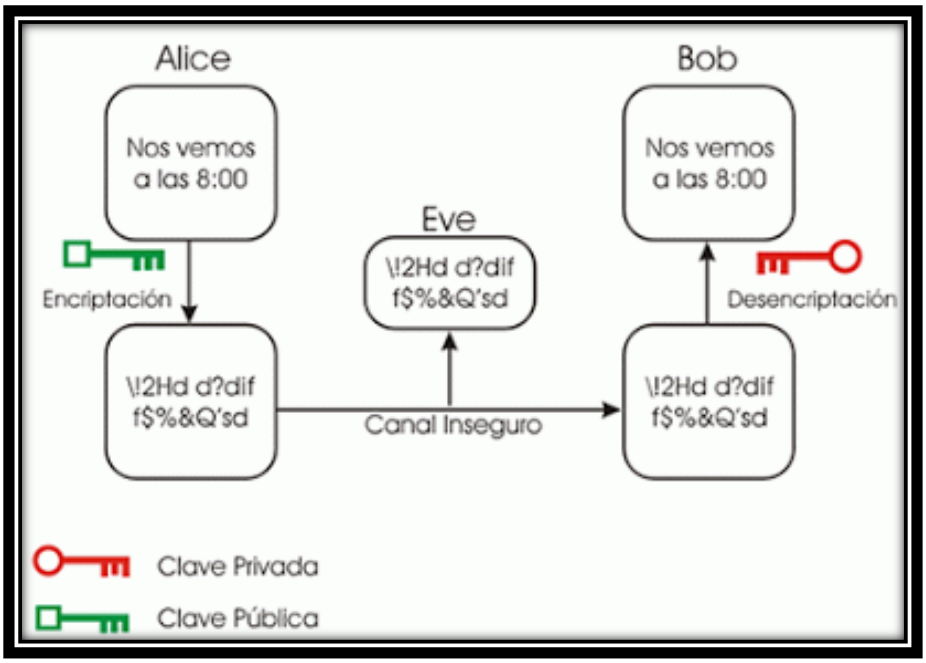

Ilustración 17 Mensaje de encriptado básico

Como podemos ver el mensaje original lo envía Alice y va dirigido a Bob, seguido de esto el mensaje se encripta y se manda, supongamos que Eve es un espía informático y trata de ver el contenido del mensaje, pero a la hora de abrir el mensaje (como no era enviado para ella y no tiene la llave adecuada para abrirlo) se da cuenta de que solo ve caracteres y símbolos y no ve un mensaje completo e íntegro. Por otro lado una vez que Bob recibe el mensaje y lo abre el sí puede ver el contenido original del mensaje tal cual fue escrito por Alice.

Aun y con estos métodos de encriptación no estamos exentos de ser víctimas de un ataque, como por ejemplo, los ataques por fuerza bruta, estos son muy costosos en tiempo computacional por lo que suelen combinarse con un ataque de diccionario.

Un ataque de diccionario es un método de cracking que consiste en intentar de averiguar una contraseña probando todas las palabras del diccionario.

Por otro lado tenemos los ataques de diccionario que tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúscula y minúscula mezcladas por números y con cualquier tipo de símbolos. Sin embargo, para la mayoría de los usuarios recordar contraseñas tan complejas resulta complicado.

3.3 Backtrack

En resumidas cuentas Backtrack no es un programa, es una distribución GNU/Linux diseñada para hacer auditorías de seguridad informática con múltiples herramientas precargadas, por lo que usarlo se compara más con usar Windows que usar un programa de este último. Dentro de Backtrack, usaremos la suite aircrack-ng, una serie de herramientas que nos permitirá obtener la clave WEP.Backtrack es libre, lo que nos permite descargarlo desde su página oficial.

http://www.backtrack-linux.org/downloads/

Una vez en la página lo podemos encontrar en KDE y Gnome (el que viene en Ubuntu y en el que se basa este pequño tutorial), que son entornos gráficos de Linux, pero de lo que vamos a utilizar todo es igual. Lo que haremos a continuación es descargar la versión ISO, y de preferencia la versión r3 que es la última. Backtrack es algo pesado, (3 gb aprox) por lo que es necesario una USB de 4 gb mínimo o un DVD donde guardarlo ya que como dije no trabajaremos sobre Windows. Al iniciar nuestra computadora no iniciará Windows o el sistema que tengan instalado, más bien iniciará Backtrack desde nuestro USB o DVD.

Es posible encontrar por la red versiones anteriores de Backtrack un poco más ligeras, sin embargo es mejor utilizar la última que tiene precargados más drivers (lo que nos ayuda ya que soporta más tarjetas de red actuales), de otra manera podemos batallar mucho intentando hacer que nos reconozca la tarjeta de red, entre otros controladores.

3.3.1 Usando Backtrack

Backtrack se puede instalar en nuestra computadora como sistema principal en todo el disco duro o en alguna partición del disco duro, sin duda la mayor ventaja de él es que (al igual que los LiveCD de Ubuntu y otras distribuciones) podemos utilizarlo sin instalarlo, algo muy útil cuando no tenemos particiones disponibles o no tenemos idea de cómo hacer una partición en un disco duro o también que solo utilizaremos el programa esporádicamente y no muy seguido

A continuación se explica cómo hacer el proceso de grabarlo en un DVD o una USB para hacerlo booteable:

- **Grabarlo en DVD** - Se hace igual que con cualquier otro DVD, lo grabamos por medio de programas como Cyberlink, Roxio, Nero o con el mismo software que trae Windows podemos grabarlo para luego arrancar de él al iniciar nuestra computadora.

- **Guardarlo en USB** - Bien, esto se vuelve un poco más complicado que grabarlo en un DVD ya que las memorias no tienen un sector de arranque y hay que cargárselo mediante un programa y un poco más a la hora de arrancar de la USB ya que hay que configurar la BIOS para ello, pero aquí va paso por paso:

Existen diferentes programas para grabar una ISO en una USB, para este pequeño tutorial se utilizará UNetbootin. Ver ilustración 18. El cual se puede descargar desde su página oficial:

http://unetbootin.sourceforge.net/

A continuación se explica cómo utilizar este programa muy sencillamente para guardar una ISO, en este caso Backtrack 5:

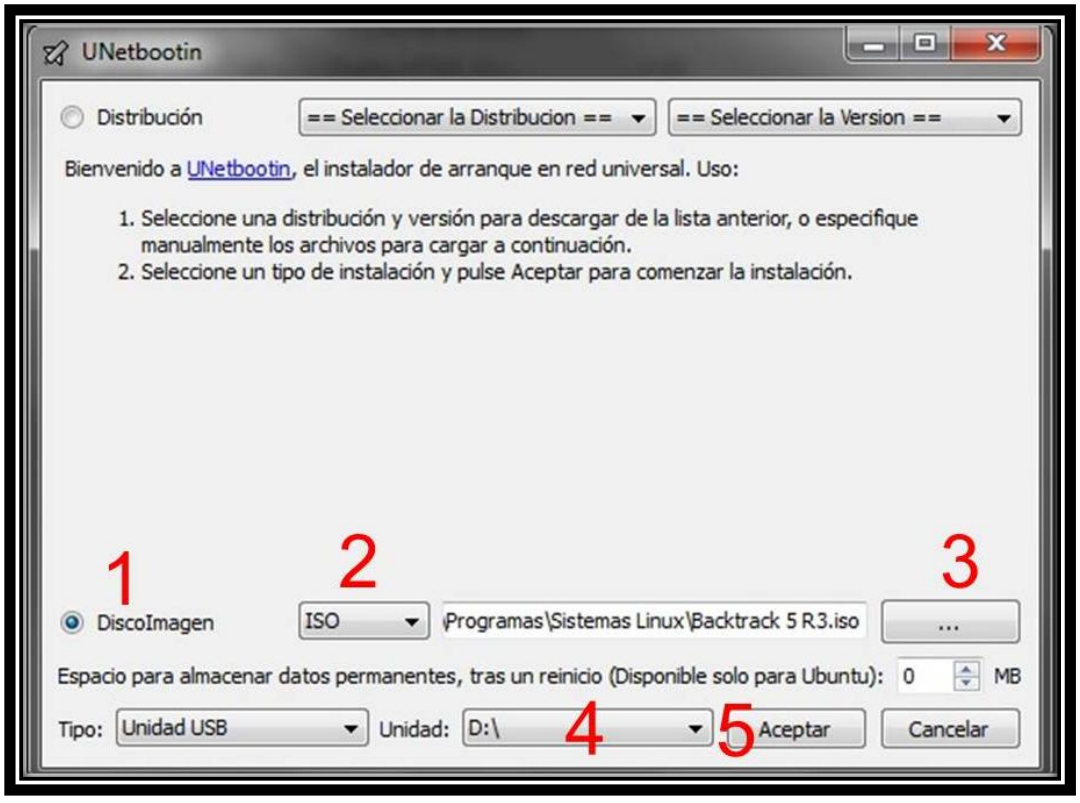

Ilustración 18 UNetbootin

1.- Seleccionamos DiscoImagen.
2.- Seleccionamos ISO.
3.- Seleccionamos la ubicación del archivo ISO de Bactrack 5 que descargamos.
4.- Seleccionamos la unidad que la computadora asignó a nuestra USB en mi caso es D:\
5.- Damos click en Aceptar.

El proceso puede ser un poco tardado, dependiendo de la capacidad de la USB y de nuestra computadora. Una vez terminado el proceso de copiado sólo damos en cerrar. Con esto ya tenemos preparado todo, es hora de utilizar Backtrack 5.

3.3.2 Descifrando la contraseña de una red con Backtrack

Bien ahora que tenemos Backtrack 5 en nuestra USB o DVD hay que iniciar desde él, para ello hay que reiniciar la computadora y:

- Seleccionar el dispositivo de arranque al iniciar la computadora.

Esto es algo muy sencillo de hacer ya que no hay que configurar nada, solo seleccionamos el dispositivo de arranque en donde tenemos Backtrack 5.

Si utilizamos el DVD probablemente no hay que configurar nada, este solo arrancara con el hecho de encender el PC y que el DVD esté en la bandeja, pero con la USB iniciaría Windows, por lo que al encender la computadora hay que presionar F12 (es la opción por dafault de la mayoría de las computadoras), una vez realizado esto debe mostrar algo como "Press F12 to select boot device" o "Presione F12 para elegir el dispositivo de arranque" entonces tendremos algo como lo siguiente imagen. Ver ilustración 19

Ilustración 19 Selección de dispositivo de arranque con F12

Aquí hay que elegir nuestra unidad de DVD o USB. Generalmente viene el tipo de dispositivo y luego alguna especificación, por ejemplo: USB: Kingston dt 101 g4

Pero no todas las computadoras tienen esta opción, entonces hay que configurar la BIOS, esto se hace normalmente presionando F2, ESC o FIN, La pc debe mostrar algo como "Press F2 to enter setup" o "Press F2 to enter Bios" una vez en la BIOS hay que ir a las configuraciones de "boot" o "arranque" y elegir como primer dispositivo de arranque o "First boot device" nuestra USB o DVD.

Es recomendable volver a dejarlo como estaba al terminar de usar Backtrack 5. Después de esto reiniciamos nuestra computadora y Backtrack 5 debería iniciar. Al iniciar Backtrack 5, lo primero que aparecerá será la siguiente pantalla: Ver ilustración 20

Ilustración 20 Captura del boot

Hay que presionar cualquier tecla y luego aparecerá esta pantalla: Ver ilustración 21

Ilustración 21 Captura de selección de modo de arranque

Seleccionamos el Default Boot - Text Mode, y después de cargar algunos controladores aparecerá la siguiente pantalla: Ver ilustración 22

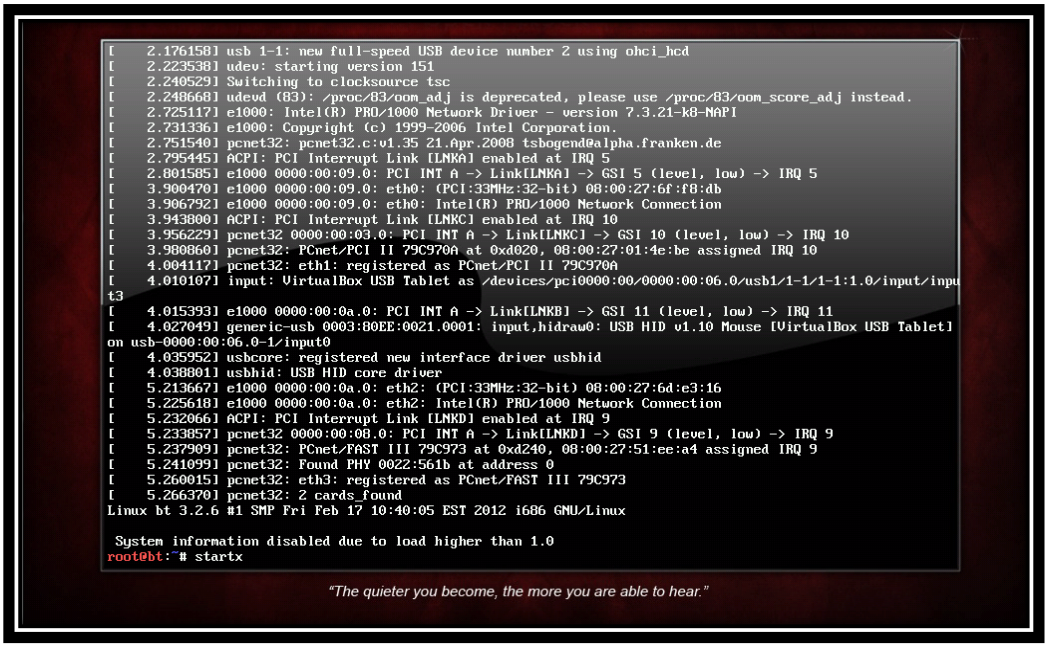

Ilustración 22 Captura de inicio de Backtrack 5 r3

Ya tenemos Backtrack 5 listo para usarse, pero para hacerlo más amigable al usuario y entrar en modo gráfico escribimos lo siguiente:

startx

Seguido de esto presionamos enter. Así iniciará el modo gráfico de Backtrack 5 r3, como se aprecia en la siguiente imagen: Ver ilustración 23

Ilustración 23 Captura del modo gráfico de Backtrack 5 r3

A simple vista se puede observar que es muy semejante a Ubuntu y lo mejor, en este punto ya estamos listos para empezar a descifrar o “crackear” la clave WEP.

El siguiente paso es preparar nuestra tarjeta de red inalámbrica para ello lo primero que hay que hacer es abrir una terminal y usar el siguiente comando:

airmon-ng

Aquí podemos ver nuestras tarjetas de red. La que utilizaremos para este tutorial es wlan0 pero también puede ser ath0 u alguna otra cosa. Ver ilustración 24

Ilustración 24 Captura del comando "airmon-ng"

Lo siguiente es poner la tarjeta en modo monitor, para ello tecleamos el siguiente comando:

airmon-ng start wlan0

En donde wlan0 es nuestra interfaz de red. Como podemos ver el modo monitor se activó en la interfaz mon0 que es la que utilizaremos de ahora en adelante. Ver ilustración 25

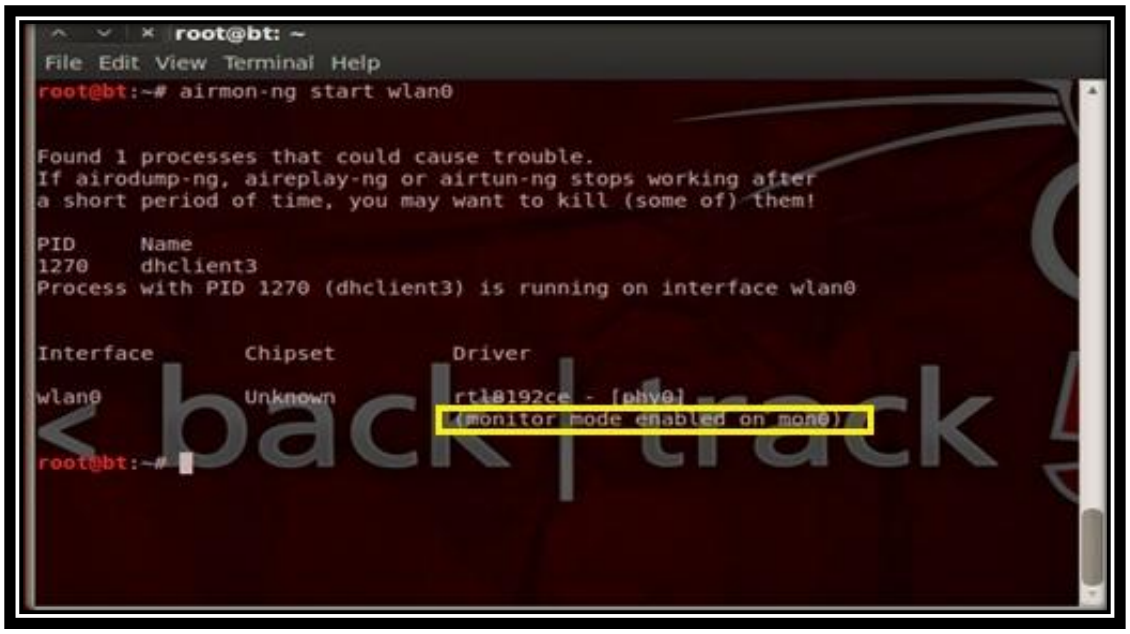

Ilustración 25 Captura del comando "airmon-ng start wlan0"

El siguiente paso es escanear las redes disponibles, para ello utilizaremos el siguiente comando:

airodump-ng mon0

Dónde:

mon0 es nuestra interfaz de red y obtendremos lo siguiente: Ver ilustración 26

Ilustración 26 Captura del comando "airodump-ng mon0"

Después de que aparezcan algunas redes o en este caso la que queremos “hackear” hay que presionar Ctrl+c para detener la búsqueda. Hay que anotar 1 el canal, y 2 la dirección MAC (BSSID) pues la utilizaremos más adelante.

El siguiente paso es comenzar a capturar los paquetes de la red, para ello utilizaremos el siguiente comando:

airodump-ng -c 1 --bssid 98:2C:BE:D8:E6:22 -w crackwep mon0

Dónde:

-c Canal en donde está la red
--bssid Dirección Mac de la red
-w Nombre del archivo en donde se guardaran los paquetes
mon0 Nuestra interfaz de red

Después de hacer este paso se abrirá una ventana parecida a la anterior, pero ahora sólo aparecerá dicha red y se estarán guardando los datos en un archivo en la carpeta root. Ver ilustración 27

Ilustración 27 Captura del comando "airodump-ng -c 1 --bssid 98:2C:BE:D8:E6:22 -w crackwep mon0"

Lo siguiente es abrir una nueva pestaña en la terminal y hacer una falsa autentificación para poder inyectar paquetes más adelante. En esta nueva pestaña utilizaremos el siguiente comando:

aireplay-ng -1 0 -a 98:2C:BE:D8:E6:22 mon0

Dónde:

-1 Flag de aireplay para la falsa autentificación, el 0 indica cada cuando se hace la falsa autentificación.

-a MAC de la red.

mon0 Nuestra interfaz de red.

Aparecerá algo así: Ver ilustración 28

Ilustración 28 Captura del comando "aireplay-ng -1 0 -a 98:2C:BE:D8:E6:22 mon0"

El siguiente paso es capturar peticiones ARP e inyectarlas para generar paquetes que nos servirán para crackear el password. Para ello utilizaremos el siguiente comando:

aireplay-ng -3 -b 98:2C:BE:D8:E6:22 mon0

Dónde:

-3 Flag de aireplay para capturar y reenviar peticiones ARP

-b MAC de la red

mon0 Nuestra interfaz de red y debe aparecer lo siguiente: Ver ilustración 29

Ilustración 29 Captura del comando "aireplay-ng -3 -b 98:2C:BE:D8:E6:22 mon0"

Que después de unos minutos debe comenzar a capturar paquetes ARP: Ver ilustración 30

Ilustración 30 Captura de paquetes ARP

En la siguiente imagen podemos ver como aumentan los Iv's que son los que necesitamos para crackear el password WEP y aparecen como #Data en la pestaña de airodump-ng: Ver ilustración 31

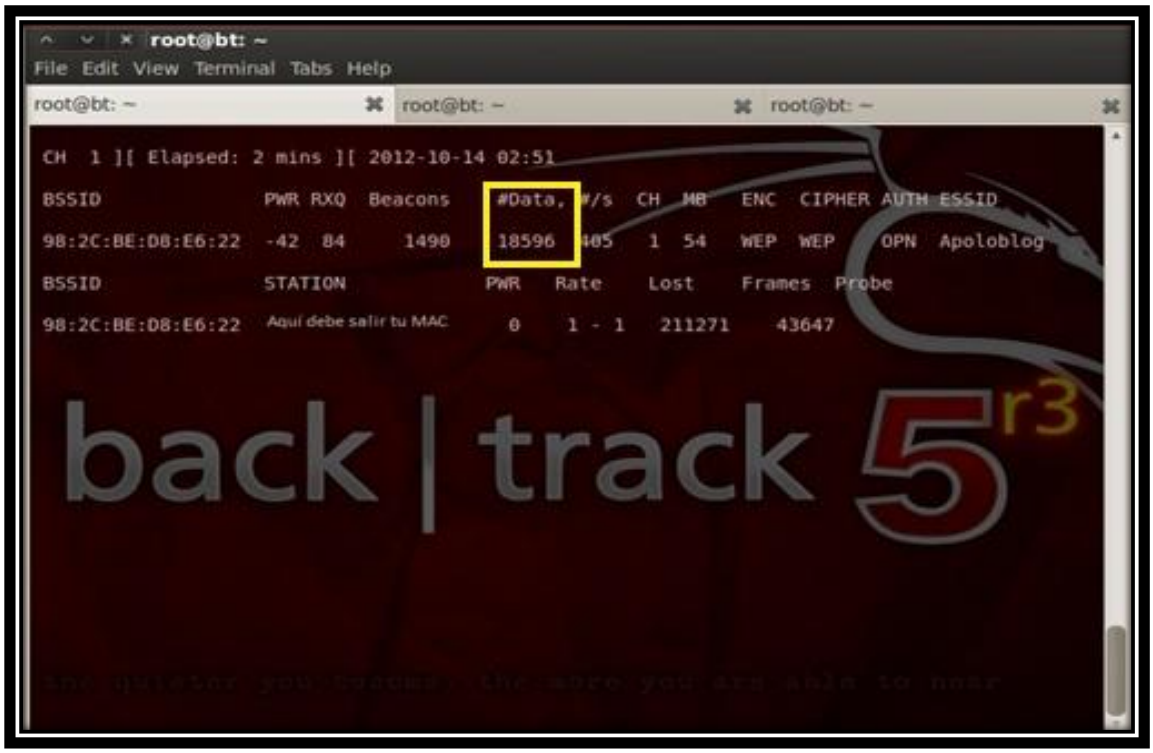

Ilustración 31 Captura de datos en la pestaña de "airodump-ng"

Normalmente con 5,000 Iv's podemos comenzar a desencriptar la clave, pero con unos 20,000 es un poco más seguro, en este caso ya tenemos poco más de 18,000 y aumentando por lo que ya podemos utilizar aircrack-ng.

Para esto vamos a utilizar el siguiente comando:

Ls

Ver ilustración 32

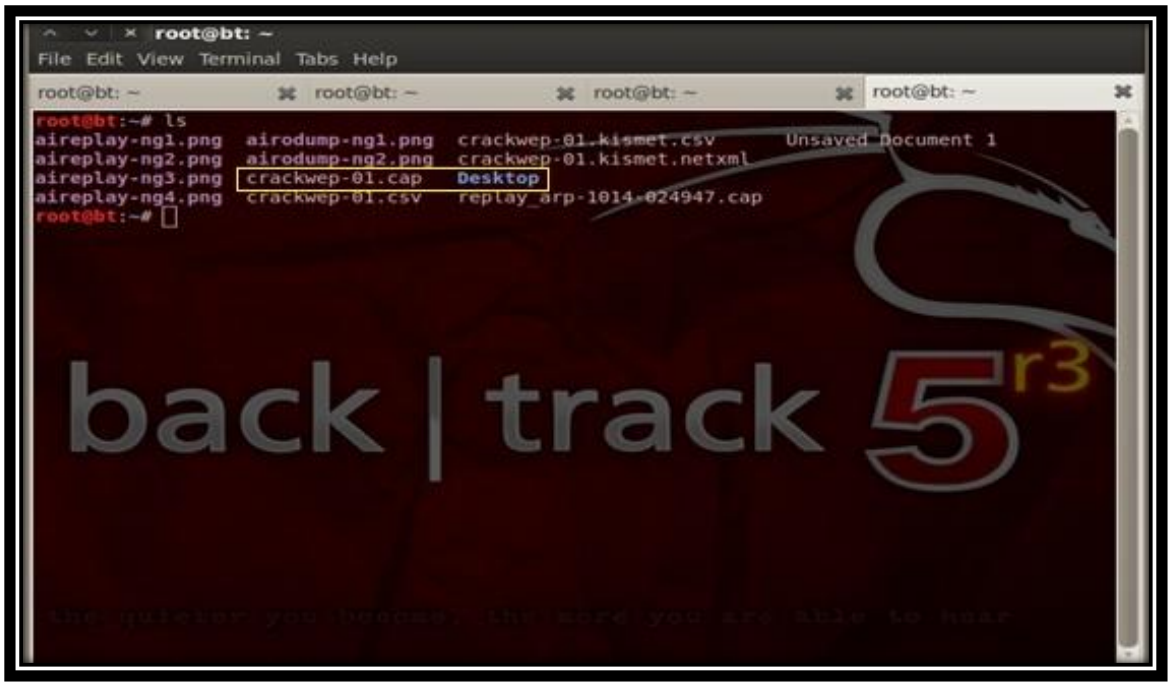

Ilustración 32 Captura del comando "ls"

Este comando nos muestra los archivos que tenemos en la carpeta root, como podemos ver están los archivos de captura que he tomado para este tutorial, así como algunos otros, de aquí el que nos servirá es el de ***crackwep-01.cap*** Que regresando un poco fue el nombre que le dimos al utilizar en ***airodump-ng*** la opción ***-w***, pero sólo habíamos puesto ***crackwep***, es por eso que utilizamos el comando ***"ls"***.

El archivo que utilizaremos siempre será el que tenga la extensión ***.cap***

Ahora que tenemos el nombre, llego la hora de usar aircrack-ng, para esto usaremos el siguiente comando:

aircrack-ng crackwep-01.cap

Dónde:

crackwep-01.cap es el nombre del archivo que creamos con airodump-ng y en donde se guardaron los paquetes de la red. Entonces aparecerá una pantalla como la siguiente: Ver ilustración 33

Ilustración 33 Captura del comando "aircrack-ng crackwep-01.cap"

Como se puede observar, obtuvimos los Iv's suficientes y a un lado de KEY FOUND aparece entre corchetes; la clave que en este caso es "0701714181" como se muestra en la imagen anterior.

Esto sería todo una vez obtenida la clave reiniciamos la computadora y sacamos el LiveCD o la USB donde tenemos Backtrack 5 r3, esto para que no vuelva a entrar y entre al sistema operativo instalado normalmente.

Cabe mencionar que hay modems con mayor seguridad que otros y durante el tutorial se pueden encontrar problemas como en la falsa autentificación. Algunos de ellos tienen un filtro MAC el cual sólo permite conectarse a las direcciones que introduzcas en el mediante su interfaz. También es necesario tener buena señal, de otra manera habrá un poco más de dificultades.

Si tenemos algunos problemas como los mencionados, solo basta reiniciar con Backtrack 5 r3 y volverlo a intentar o en su debido caso moverse a un lugar donde se tenga mejor señal de la red a la que queremos atacar o “hackear”.

3.4 Dentro de una red

Una vez dentro de una red ya sea propia o ajena, lo que sigue ya es propio del usuario aunque se pueden hacer varias cosas como explico a continuación; una de las cosas que se pueden hacer es cambiar el nombre de la red el llamado SSID, este es el nombre con que se da a conocer nuestra red a las demás computadoras o equipos inteligentes.

Otra de las cosas importantes que se puede hacer es cambiar la contraseña del modem, recomiendo que en este punto si es modem propio cambiar la contraseña a una más segura, más adelante explicare esto más detalladamente; por otro lado también se puede cambiar el canal de transmisión de la red y el tipo de seguridad de la misma ya sea TKIP, AES, PSK, etc.

Estando dentro del modem podemos observar los equipos conectados a esa red y podemos dar privilegios a una computadora o en su debido caso negarle el acceso al modem, así como deshabilitar o habilitar la red Wi-Fi.

Capítulo 4

4.0 Mantener segura nuestra red Wi-Fi

Las redes Wi-fi son cada vez más utilizadas y todos los ordenadores y/o dispositivos tales como tabletas, smartphones, impresoras, etc., modernos están preparados para trabajar con este tipo de red sin dificultad alguna. Una de las cosas a considerar es que cada día más y más usuarios optan por tener una red inalámbrica y las mismas empresas que prestan este servicio de internet ofrecen este tipo de red, esto ha llevado a un gran crecimiento en el uso de redes Wi-Fi.

El mayor problema de seguridad de las redes Wi-Fi viene dado por su dispersión espacial. No está limitada a un área, a un cable o una fibra óptica, ni tienen puntos concretos de acceso o conexión, si no que se expande y es accesible desde cualquier punto dentro de su radio de cobertura. Esto hace muy vulnerables a las redes inalámbricas pues la seguridad física de dichas redes es difícil de asegurar.

La posibilidad del acceso o monitorización de los datos es una amenaza muy real. Es por esta razón que todos los equipos permiten la encriptación de las comunicaciones mediante diversos algoritmos, que permiten tanto autenticar a los usuarios para evitar accesos no autorizados, como evitar la captura del tráfico de la red por sistemas ajenos a esta.

Otra de las consecuencias de ser una red vía radio es la influencia de otras fuentes radioeléctricas, ya sean otras redes Wi-Fi, equipos radio que trabajen en la misma banda o aparatos de distinta índole que generen interferencias. Es por tanto posible la generación de una interferencia premeditada que bloquee la red Wi-Fi y evite el funcionamiento de esta.

Es por esta razón que debemos de tener nuestra red lo más segura posible, lo que podemos hacer es pasar desapercibidos o hacer más complicado el ataque, tal vez de esta manera podamos evitar que desistan.

4.1 Firewall

Un Firewall es un dispositivo que funciona como cortafuegos o barrera entre redes, permitiendo o denegando las transmisiones de una red a la otra.

Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial, de igual forma esta barrera examina todos y cada uno de los paquetes de información que tratan de atravesarlo. En función de reglas previamente establecidas, el Firewall decide qué paquetes deben pasar y cuáles deben ser bloqueados.

Un Firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Básicamente un Firewall es una especie de barrera delante de nuestro equipo. Ver ilustración 34

Muchos tipos de Firewalls son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los diferentes tipos de código malicioso como caballos de Troya, virus y gusanos, entre otros, sean efectivos. El Firewall actúa de intermediario entre nuestro equipo (o nuestra red local) e Internet, filtrando el tráfico que pasa por él.

Ilustración 34 Representación de un Firewall

Dependiendo del Firewall que estemos utilizando, también podremos aprobar algunos accesos a la red local desde Internet, si el usuario se ha validado como usuario de la red local. Existen 3 tipos de Firewalls:

4.1.1 Firewalls de aplicación

Tienen un costo pequeño y son una buena elección cuando sólo se utiliza una PC. Su instalación y actualización es sencilla, pues se trata de una aplicación de seguridad, como lo sería un antivirus; de hecho, muchos antivirus lo traen por default e incluso el propio Sistema Operativo Windows poseen Firewalls para utilizar.

4.1.2 Enrutadores de hardware

Su principal función es disfrazar la dirección y puertos de la PC a los intrusos. Suelen tener cuatro puertos de red para conexión mediante cableado.

4.1.3 Firewalls dedicados

Son más caros y complejos de manejar en el mantenimiento y actualización. Los Firewalls de hardware son más indicados en empresas y grandes corporaciones que tienen múltiples computadoras conectadas. También suelen utilizarse en aquellas empresas que prestan servicios de hosting y necesitan seguridad en los servidores.

Firewall de Aplicación

El más usado en empresas pequeñas y hogares comúnmente es el **Firewall de aplicación**, a continuación se explica de forma general como activarlo y se dan a conocer algunas características del mismo. Posiblemente el hecho de que Microsoft incorpore en tu Sistema Operativo Windows un cortafuegos (Firewall), sea motivo de confianza para no tener que desactivarlo y utilizar otro, así que lo veremos en su versión de Windows 7.

El Firewall de Windows 7 al estar incorporado en el propio sistema operativo de Microsoft ofrece como ventaja principal una perfecta integración y gestión de los recursos del propio sistema.

Para la localización del Firewall de Windows 7 sólo tendrás que seguir los siguientes pasos: **Inicio > Panel de Control > Sistema y seguridad** y aparecerá la siguiente pantalla donde podrás acceder a las funcionalidades del Firewall de Windows. Ver ilustración 35

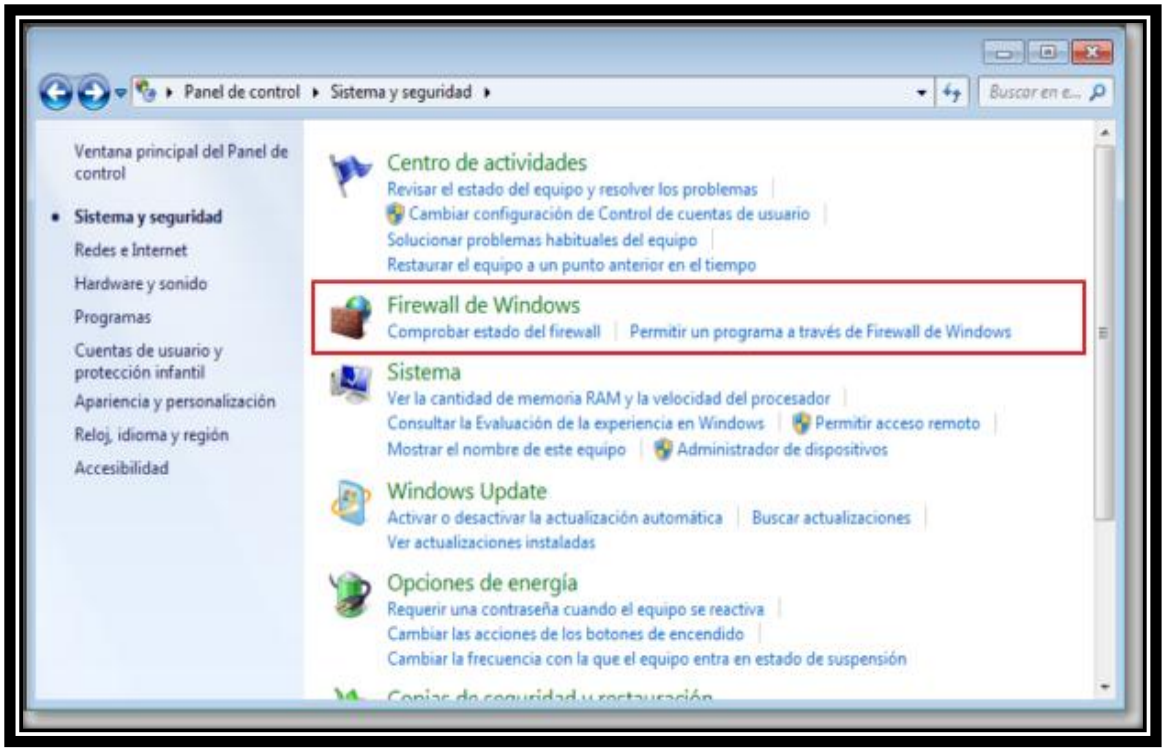

Ilustración 35 Panel de control - Sistema y seguridad - Firewall de Windows

Como se habrán dado cuenta llegar hasta este paso es demasiado sencillo, de igual forma con la configuración del Firewall no es nada del otro mundo, a continuación daremos click donde dice **Firewall de Windows**, el cual nos mostrará el submenú de opciones y la visualización de la configuración del Firewall. Ver ilustración 36

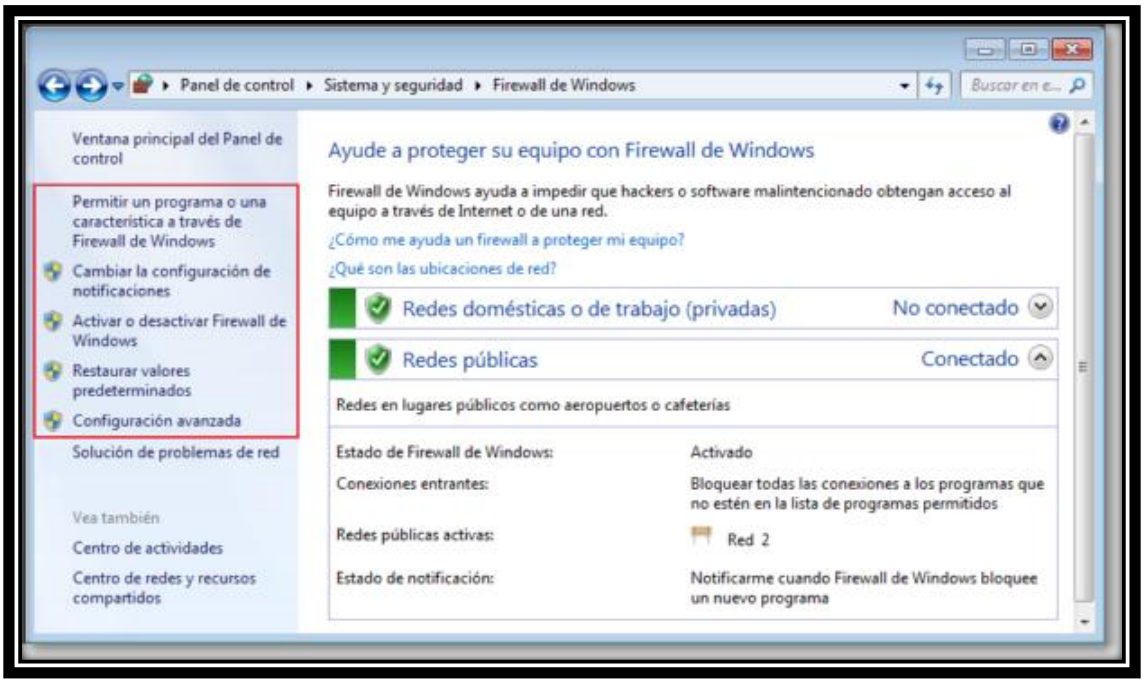

Ilustración 36 Submenú del Firewall de Windows

Las opciones que muestra son las siguientes:

La primera opción es la configuración de los **permitir un programa o una característica a través de Firewall de Windows**.

Esta opción nos permite ver los detalles de cada uno de ellos (programas instalados en nuestra computadora), activar el cambio de configuración o realizar nuevos permisos de otros programas que queramos añadir.

En la segunda y tercera opción nos permite **Cambiar la configuración de notificaciones** o **Activar o desactivar Firewall de Windows**. Ambas opciones de este submenú nos llevan a la personalización de la configuración para elegir, activando o desactivando sus opciones ya explicadas anteriormente. La configuración que nos muestra gráficamente se representa como **Firewall activado** , **Firewall desactivado** o **Bloqueo de todas las conexiones entrantes** . Ver ilustración 37

Ilustración 37 Configuración del Firewall de Windows

La cuarta opción es **Restaurar valores predeterminados**, esta opción lo que hace es que nos devolverá a la configuración por default del sistema.

La quinta y última opción del menú de Firewall de Windows es el acceso a la **Configuración avanzada** que nos permitirá dar una gestión más personalizada de cada una de las reglas establecidas y nos permite, además de tener una visión más pormenorizada de cada una de ellas, habilitarlas o deshabilitarlas, cortarlas, eliminarlas,.... Esta opción es para usuarios más avanzados en el tema de Firewall (no recomendado a usuarios inexpertos en el tema).

Como nota importante cabe mencionar que cada vez que Windows intercepte una conexión o programa que no tenga contemplado en sus permisos nos mandara un aviso si así se lo hemos configurado en las opciones anteriores. Ver ilustración 38

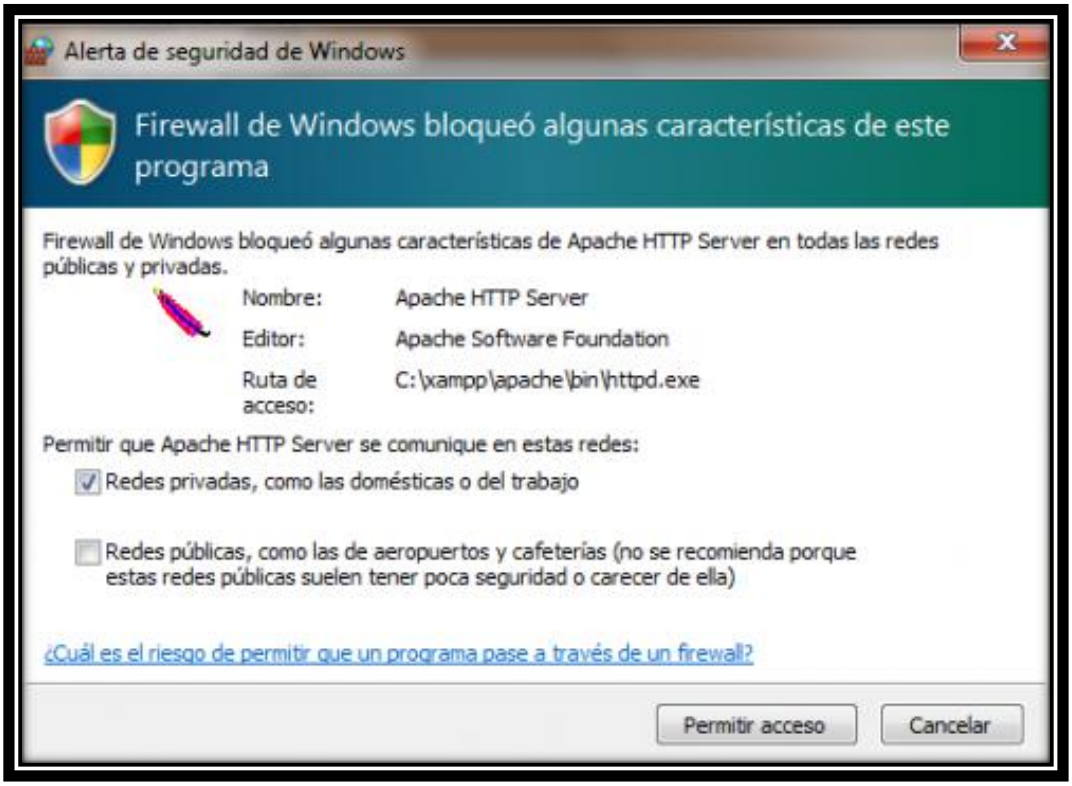

Ilustración 38 Permisos del Firewall de Windows

4.2 Buenas prácticas de uso en las redes

Cando se piensa en vulnerabilidad de una red Wi-Fi se considera, como lo hemos hecho hasta ahora, la posibilidad de que un cliente no autorizado acceda a datos de la red. Sin embargo existe otro peligro: la inclusión de un punto de acceso no autorizado en la red.

Un atacante puede añadir un punto de acceso que anuncie el mismo nombre de red, confundiendo así a algunos clientes que se podrán llegar a conectar a él en vez de a la red legal. Dependiendo de la elaboración de la suplantación, el cliente puede llegar a revelar datos y claves importantes.

Por ello es que la seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito.

Por ello, se dan a conocer una serie de recomendaciones para tener en cuenta a la hora de mantener segura una red inalámbrica:

4.2.1 Cambiar frecuentemente el password y/o contraseña

Esto es básico y uno de los puntos más importantes en cuestiones de seguridad de una red inalámbrica, nunca se debe dejar la contraseña que trae por default él Router, normalmente esta contraseña es la misma que la contraseña de administrador. Esto implica que si alguien descubre la contraseña puede tener acceso a administrar el equipo y hacer una serie de cambios en él.

La contraseña es uno de los factores más importantes en cuestión de seguridad, la recomendación es usar contraseñas mínimas de 8 caracteres y que contengan letras tanto mayúsculas como minúsculas de igual forma poner números y símbolos.

Evitar contraseñas obvias o muy fáciles de encontrar como por ejemplo “qwerty0123” o “abc123”, trate de usar contraseñas un poco más complejas por ejemplo “Dragon-fuego@548” o “cAsa$98/solA”.

“Existen otros trucos para recordar claves aparentemente complejas. Por ejemplo: reemplazar letras por números o signos (´<0m0k#O?´ en vez de ´¿Cómo que no?´), elegir una palabra sin sentido, aunque pronunciable (´m1k0f3´ por ´micofe´) o utilizar acrónimos e frases no populares (Np6+x1N por ´No puedo beber más por las noches´).” (Gómez, 2011).

Lo más importante de todo, es que para evitar accesos no autorizados a una red, es imprescindible no compartir la contraseña con nadie solo deberá saberlo el propietario de la red y/o el administrador de la misma, así como cambiarla frecuentemente, al menos dos veces por mes, si es de misión crítica o cada seis meses si no lo es.

4.2.2 Activar encriptación

Esto es en pocas palabras cambiar el tipo de seguridad de nuestra red. Es recomendable usar el cifrado WPA ya que, como ya se mencionó en capítulos anteriores, es más seguro y más fiable que el cifrado WEP.

4.2.3 Cambiar el nombre del SSID

Este es el nombre con el que puedes ver tu red de forma inalámbrica para conectarte, así es como identificas que efectivamente es tu red, cuantos infinitum han vistió por todos lados, estos son equipos a los que no se les ha cambiado el nombre que traen por default por ejemplo “INFINITUM2F014” y probablemente tampoco han cambiado la contraseña del mismo.

En este punto es recomendable cambiar el nombre de nuestra red (SSID) por cualquier otro que les guste, cabe mencionar que para despistar un poco a los que quieran entrar a nuestra red, es preferible que el nombre no dé a conocer el modelo del Router, ni el nombre de la empresa o el nombre del proveedor de servicio, por ejemplo: si nuestra empresa se llama “Kesitos S.A de C.V” no poner como nombre de la red “Kesitos”.

Otra alternativa, aunque no es muy recomendable hacerlo ya que podemos olvidar el nombre correcto de nuestra red, es ocultar el nombre de la SSID, esto quiere decir que estará visible nuestra red pero no se mostrara el nombre de la misma. De esta forma cualquiera que se quiera conectar deberá saberse el nombre de nuestra red.

4.2.4 Habilitar filtrado por Mac

Esta es una de las funcionalidades más seguras ya que solo las direcciones Mac que des de alta en tu dispositivo tendrán acceso, para poder hacer esto tienes que saber que dispositivos se conectarán y hacer un listado de los dispositivos permitidos en tu Router.

La dirección MAC es una dirección de nivel 2 que lleva la tarjeta de red Wi-Fi grabada de fábrica (análoga a la dirección MAC-Ethernet), el problema con este método es que si tienes una visita y quiere tener acceso necesitaras entrar a tu Router e incluir sus direcciones Mac para que tengan acceso, por otro lado el método no es infalible ya que existen tarjetas de red que permiten el cambio de la dirección MAC, y en ese caso sería posible para un atacante de nuestra red, asignarle una dirección válida de alguno de nuestros equipos y evitar esta medida de seguridad.

Pero para ello, el atacante, debería conocer la dirección MAC de alguno de nuestros equipos, lo cual si las medidas de seguridad física e informática están correctamente implementadas en nuestra empresa y hogares no resultará fácil.

4.2.5 Establecer un límite de dispositivos en la red

Esto es simplemente saber con cuantos dispositivos cuento y cuántos de ellos pueden conectarse a la vez de forma inalámbrica y alámbrica. En una red del hogar, el número no debe ser muy alto aproximadamente menor o igual a 5, a diferencia de una pequeña empresa que pueda tener más de 15 equipos conectados al mismo tiempo, esto se define por políticas de la empresa y esta decide quienes y cuáles son los dispositivos que se conectaran a su red.

4.2.6 Revisar periódicamente los dispositivos conectados

Esta práctica te ayuda a ver si algún dispositivo que no autorizaste está conectado o lo estuvo, ya que los dispositivos que se conectaron en algún momento permanecen visibles en la configuración aun cuando ya se desconectaron, los Routers más nuevos tienen la funcionalidad de identificar el tipo de dispositivo conectado con diferentes iconos para que sepa si estuvo conectada una PC o un dispositivo móvil en tu Router, incluso saber si era una Mac o equipo Windows.

De esta forma logramos tener un control superior de nuestro Router y de igual forma estamos pendientes del acceso a nuestra red. Si encontramos un dispositivo el cual no conocemos y como ya mencione esta o estuvo conectado a nuestra red, entonces eso quiere decir que en algún punto de nuestra configuración de seguridad del Router está débil o habrá que reforzar esa parte.

4.2.7 Instalación de un Firewall

Respecto a este punto ya mencionado habrá que utilizar el tipo de Firewall acorde a nuestras necesidades. El acceso de los clientes Wi-Fi a la red cableada debería ser gestionado por un Firewall, ya sea actuando de puente entre las correspondientes VLANs o como elemento físico de control, interponiéndose en el flujo de tráfico Wi-Fi. Esto propicia un correcto funcionamiento de la red y por ende una mayor seguridad.

En cualquier arquitectura de red, incluir un Firewall nos permitirá implementar políticas de acceso seguras y complejas que aseguren que, aunque algún intruso hubiese conseguido conectarse a la red inalámbrica de forma no autorizada o permitida, no progrese hasta tener acceso a datos sensibles.

4.2.8 Mantén actualizado tu Router

Los Routers más recientes te avisarán cuando hay una actualización para tu equipo, prácticamente lo que se hace aquí será dar click para que se actualice nuestro dispositivo con las mejoras más actuales y disponibles, algunos se actualizan automáticamente, pero no está de más revisarlo periódicamente ya que estas actualizaciones podrían estar relacionadas con temas de seguridad en la red o mejoras en el desempeño del Router.

4.2.9 Cambiar todas las claves regularmente

Este es otro punto muy importante ya que la mayoría de las personas hacen caso omiso de esto y dejan la contraseña que viene por default o en su debido caso jamás vuelven a cambiar la contraseña que asignaron.

Tanto las claves de acceso a nuestra red, como las de la administración del AP (Access Point) o Router deben de ser cambiadas constantemente, recomiendo hacer esta práctica aproximadamente cada mes o cada dos meses, de esta forma si alguien intenta acceder a nuestra red le sea complicado ya que constantemente se está renovando la contraseña de acceso.

4.2.10 Desactivar el AP

Es recomendable que cuando no se utilice el Router por cuestión de que se presente una situación de salir por unos días del domicilio donde se encuentra instalada la red (ya sea por motivos de trabajo o por vacaciones) y/o empresa (por motivo de puentes, vacaciones o días de asueto), o no se esté utilizando en el momento se apague, de esta forma y por razones obvias nadie tendrá acceso a nuestro Router.

Cabe destacar que no es muy recomendable hacer esta práctica en empresas cuya función se basa en el manejo de datos con otras empresas, ya que al apagar el Router se perderán grandes cantidades de información importantes para ambas o múltiples empresas y de igual forma se perderá comunicación con ellas.

Normalmente nadie cambia estos datos en su red inalámbrica y esto las hace muy fáciles de hackear, en aproximadamente 15 minutos un usuario con conocimientos moderados podría obtener la llave de acceso a tu Router y el siguiente paso es tu información personal.

Siguiendo estas recomendaciones podemos hacer que nuestra red inalámbrica sea más segura y podemos hacer las cosas más difíciles a cualquiera que intente entrar en ella.

Ninguno de estos métodos es 100% seguro, pero el uso de varios o todos estos métodos en conjunto nos ayudará a tener más seguridad y que sea más difícil que alguien logre descifrar tu clave de acceso y/o tener acceso de forma no autorizada a nuestro Router.

Si por alguna razón se te hace difícil modificar estos parámetros en tu Router, la mejor recomendación es llamar al prestador del servicio de internet que tengamos en nuestro hogar o empresa, para que ellos nos vallan guiando de manera fácil y sencilla en la configuración de estos parámetros sin temor a des configurar o alterar datos.

Aun así y con todas estas medidas de seguridad no estamos fuera de un ataque o alguna infiltración a nuestro Router y/o Modem.

Por ello empresas como Cisco, Lynksys, Motorola, entre otras, están trabajando arduamente para brindarnos la mayor seguridad posible en sus AP’s que ofrecen y cada día los van mejorando y actualizando conforme avanza la tecnología.

Conclusiones

La tecnología inalámbrica (Wi-Fi) sin duda facilita la vida cotidiana de las personas. Gracias a esta, los usuarios ya no dependen de un cable para poder utilizar servicios en Internet. Hay que evaluar aspectos relativos a los límites de la WLAN, tanto desde el punto de vista de la cobertura de la señal, como del control de los dispositivos en dicho entorno, evitando los puntos de acceso no autorizados.

Así mismo hay que tener en cuenta los avances en los estándares que mejoran la seguridad de estas instalaciones, y por supuesto, educar a los usuarios en prácticas que les ahorren disgustos como por ejemplo, no habilitar una tarjeta en modo ad-hoc, o no dejar configurado el cliente WIFI para que se conecte a cualquier WLAN abierta.

No obstante, esta tecnología también permite a terceros interceptar la información que el usuario transmite de forma más sencilla que en redes cableadas. Esto es más complejo si se tiene en cuenta que existe una extensa cantidad de redes Wi-Fi públicas e inseguras.

Como se explicó en este trabajo, hay diversas formas de romper la seguridad de una red inalámbrica mediante algunos programas y software, esto nos indica que cualquier persona con conocimientos básicos en redes y teniendo las herramientas necesarias puede entrar a nuestra red sin ser detectado.

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

Actualmente el único ataque contra WPA es la fuerza bruta, lo que implica que sólo será realmente efectivo el ataque, si la contraseña que usamos está basada en diccionario o es muy simple.

Cabe mencionar que en la práctica si la clave es WPA, compleja y larga y además tiene algún tipo de seguridad extra, como filtrado por MAC, o DHCP desactivado, prácticamente estamos seguros que el acceso a nuestra red sería tan complejo, que se necesitaría mucho tiempo y sin garantías de que se podría conseguir la contraseña, lo que haría desistir a cualquiera.

Sea por cable o por el aire, la información del usuarios puede estar expuesta; y es siempre necesario considerar la mejor forma de protegerla.

Bibliografía

- *hacking-etico.org; Seguridad Informática*. (2013). Recuperado el 02 de 04 de 2014, de http://www.hacking-etico.org/
- A., B. (2007). *Fundamentos de redes.* México: McGrawHill.
- Arboledas, D. (2013). *Backtrack 5; hacking de redes inalámbricas.* España: RA-MA.
- Ariganello, E. (2011). *Redes Cisco; Guía de estudio para la certificación CCNA 640-802.* México: Alfaomega.
- Caldarelli, G., & Catanzaro, M. (2014). *Redes; Una breve introducción.* España: Alianza editorial.
- Callejas, R. A. (2013). *Informática.* México: Grupo Editorial Patria.
- Carballar, J. A. (2011). *Wi-Fi; Como construir una red inalámbrica.* México: Alfaomega.

- CERT, U. (08 de 2009). *Firewalls personales.* Recuperado el 03 de 03 de 2014, de http://www.seguridad.unam.mx/descarga.dsc?arch=422
- *CISCO.com*. (s.f.). Recuperado el 17 de 03 de 2014, de http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html
- Deitel, P. J., & Deitel, H. M. (2013). *Como programar en JAVA .* España: ADDISON-WESLEY.
- *galeon.com.* (s.f.). Recuperado el 11 de 02 de 2014, de http://redesinl.galeon.com/aficiones1340364.html
- Galindo, L. H. (2012). *Bases de Datos.* México: RA-MA.
- Gómez, Á. (2011). *Enciclopedia de la seguridad informática.* España: RA-MA.
- Gómez, Á. (2011). *Redes Cisco; Guía de estudio para la ertificación CCNA 640-802.* México: Alfaomega.
- Herradon, A. M. (2014). *Informática básica para mayores.* España: RA-MA.
- Katz, M. (2013). *Redes y Seguridad.* España: S.A. Marcombo.
- Kenneth C., L. J. (2012). *Sistemas de información gerencial.* México: Pearson.
- Kurose James, R. K. (2010). *Redes de computadoras; Un enfoque descendente.* España: Pearson.
- López, J. G., & Nuñez, P. G. (2014). *Hackers Aprende a atacar y a defenderte.* México: RA-MA.
- Mayers, M. (2010). *Redes : administración y mantenimiento.* España: Anaya Multimedia.
- Montalban, I. L. (2014). *Bases de Datos.* México: Garceta Grupo Editorial.

- Rysavy, P. (25 de 06 de 2013). *Network Computing.* Recuperado el 18 de 02 de 2014, de http://www.networkcomputing.com/netdesign/wireless1.html
- Sánchez, J. L. (2011). *Programación C++.* España: Anaya Multimedia.
- Silberschatz, A. (2014). *Fundamentos de Bases de Datos.* España: S.A. MCGRAW-HILL / INTERAMERICANA DE ESPAÑA.
- Tanenbaum, A. (2012). *Redes de Computadoras .* New Jersey: Pearson.
- Trigo, V., & Martin, A. C. (2009). *Windows 7; Informática para torpes.* España: Anaya Multimedia.
- Velasco, M. A., Serrano, D. C., & Shamsafar, A. (2013). *El libro del Hacker.* México: Anaya Multimedia.
- Vergara, K. (06 de 05 de 2007). *bloginformatico.com.* Recuperado el 08 de 03 de 2014, de http://www.bloginformatico.com/topologia-de-red.php
- Vieites, A. G., & Rey, C. S. (2012). *Sistemas de información herramientas prácticas para la gestión empresarial* (4 ed.). México: Alfaomega.