UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CAMPUS ACATLAN

Seguridad en la transmisión de información a través de una red inalámbrica en los sistemas de la ENEP Acatlán.

TESINA

QUE PARA OBTENER EL TITULO DE:

Licenciado en Matemáticas Aplicadas y Computación.

Presenta.

Luis Alberto Ayala López

Asesor. M. en C. Georgina Eslava García

Santa Cruz Acatlán, Edo. de México

MAYO 2006

AGRADECIMIENTOS.

A la Universidad Nacional Autónoma de México.

Quiero agradecer a la máxima casa de estudios por haberme brindado la oportunidad de pertenecer a ella como estudiante. Es un orgullo formar parte de tan honorable institución, a través de la cual recibí una preparación intelectual y personal inigualable a las demás.

A la Facultad de Estudios Superiores Acatlán.

Por su puesto quiero agradecer de manera especial a la FES Acatlán de la cual me siento muy orgulloso de ser egresado.

A mi asesora la Maestra Georgina Eslava García.

Por el tiempo y la atención ofrecida para la realización de este trabajo. Le estaré eternamente agradecido.

A mis Sinodales.

La licenciada Catalina Solís Diego, el licenciado Juan Torres Lovera, el Actuario Hugo Reyes Martínez , el licenciado Ernesto González Tenorio y la Maestra Georgina Eslava García. Por el voto de confianza ofrecido al trabajo realizado.

A mis Padres.

Por el apoyo incondicional y estimulo constante para la elaboración y culminación de este trabajo en todo momento. (Victor Ayala Pérez y Olga López Olivares)

INDICE

PROLOGO

El interés general de este trabajo es exponer de manera clara y sencilla un tema que es actual y muy importante en nuestro dìa; como lo es la seguridad dentro de una red inalámbrica.

En estos últimos años es muy común emplear el concepto de redes y es muy probable que intuitivamente se asocie con la llamada autopista de la información, aunque a su vez sabemos que estos sistemas constan de muchas partes para poder lograr el objetivo para el que se diseñaron.

En este trabajo proporcionaremos algunas formas y métodos basados en conceptos básicos de computación y matemáticos que se llevan a cabo en el envío y recepción de información de manera mas segura y confiable en una red sin cables.

Por lo tanto daremos a conocer lo que es una red, los componentes las diferentes topologías que existen y sobre todo, sacarle mayor provecho a la información transmitida para que sea lo mas segura posible. Para lograrlo se requerirá de conocimientos clásicos de computación, algunos aspectos técnicos y normas básicas a seguir, todo en función de redes y la seguridad imperante dentro de ellas.

Conocer y entender de este tema es bastante sencillo, ya que con el tiempo nos empezaremos a familiarizar con los términos y el uso de la misma, debido al auge y al uso cotidiano directo o indirecto de las redes, por lo tanto no será necesario tener una ingeniería o carrera técnica para poder manejar los elementos básicos de una red.

INTRODUCCIÓN.

En la actualidad estamos acostumbrados a tomar ciertas precauciones o actitudes, que consideramos lógicas o de sentido común, para proteger nuestros intereses o aquello que consideramos importante. Existen un sin fín de pequeñas acciones tendientes a procurarnos una mayor seguridad.

La incorporación de las nuevas tecnologías en nuestras vidas nos encamina a un nuevo mundo virtual fantástico, pero también nos plantea nuevas situaciones que debemos conocer y afrontar.

Uno de los temas que tendemos a olvidar o a dejar un poco de lado al incorporar la información a la red es la seguridad, un aspecto de seria consideración. Algo que nos debe hacer reflexionar es la seguridad en nuestra red.

Las diversas situaciones en las que nos podemos ver envueltos por no tener prevista la seguridad en nuestra conexión puede llegar a ser realmente preocupante, por ello, el recomendar algunas medidas de seguridad que garanticen la privacidad y protección de la información, de los sistemas de la FES Acatlan, transmitidas a través de una red inalámbrica será de vital importancia, incluso aunque no lo percibamos en ese momento a tal grado que ni siquiera nos enteramos que la información esta teniendo algún otro tipo de manipulación.

La libertad que proporcionan los dispositivos inalámbricos es su principal ventaja e, irónicamente, también su principal problema. Al contrario de las redes cableadas, un intruso no necesita acceso físico a nuestro edificio u oficina para intentar asaltar la red interna. Las señales de radio que utilizan los dispositivos de red inalámbricos navegan con libertad absoluta a través del aire, y por lo tanto están al alcance de cualquiera que tenga capacidad para interceptarlas. Debido a ello, a la hora de afrontar el reto de la movilidad, es imprescindible tener estos aspectos en mente y tomar las medidas adecuadas, por lo tanto el objetivo de este trabajo es proporcionar recomendaciones con base en un análisis de seguridad ya que la facultad actualmente esta sustentada por una red híbrida con algunos puntos de acceso y filtrado inicial conocido como pared de fuego (firewall) y que por lo tanto necesita una mayor seguridad previendo el crecimiento de información y el manejo confidencial de información garantizando la protección de la información de los sistemas de la FES Acatlan durante su transmisión.

El trabajo esta elaborado en cuatro capítulos, abordando en primera instancia el concepto de trabajo en redes, ya que es probablemente tan antiguo como lo es el de las telecomunicaciones

Por supuesto, la humanidad ha avanzado En la actualidad, contamos con computadoras que se comunican a traves de una colección de cables, fibra óptica, microondas, etc., Se hará referencia a los conceptos y métodos que son utilizados para llevar a cabo todo esto. Sin embargo, dejaremos de lado el tema de los cables

Una red, como una colección de *nodos* (del inglés hosts), capaces de comunicarse entre sí, a veces confiando en los servicios de un número determinado de máquinas que se encargan de transmitir datos entre quienes que lo demanden. Los nodos son casi siempre computadoras, pero no necesariamente; se puede pensar, sin equivocación, en terminales X o impresoras inteligentes o tontas como nodos. Por otro lado, a las pequeñas aglomeraciones de éstos, se las denomina *sitios*, (sites).

Así, los protocolos usados en las redes de computadoras no son más que reglas muy estrictas de intercambio de mensajes entre dos o más servidores.

Em el siguiente capitulo notaremos que las redes inalámbricas de alta velocidad pueden proporcionar beneficios de conectividad en red sin las restricciones de estar ligadas a una ubicación o tejidas por cables. Existen muchos escenarios en donde esta puede ser una alternativa interesante, incluyendo los siguientes:

Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de cuándo una red inalámbrica puede tener sentido o hasta ser requerida. Algunos tipos de edificios o códigos de construcción pueden prohibir el uso de cables, haciendo de las redes inalámbricas una alternativa importante.

Dentro del Capitulo 3 se muestra como en una red cableada existe una seguridad inherente en el hecho de que un ladrón potencial de datos tiene que tener acceso a la red a través de una conexión cableada, lo que normalmente quiere decir que necesita un acceso físico a la planta de cables de la red. Además de este acceso físico, se pueden estratificar otros mecanismos de seguridad.

Cuando la red ya no está formada por cables, la libertad adquirida por los usuarios de la red también puede ampliarse al robo potencial de datos. Ahora, la red puede estar disponible en los pasillos, áreas inseguras de espera, hasta afuera de un edificio. En un ambiente doméstico (en casa), su red puede ampliarse a las casas de sus vecinos si la red no adopta mecanismos adecuados de seguridad o si no se usa apropiadamente.

Desde su creación, la red inalámbrica ha proporcionado algunos mecanismos básicos de seguridad para que esta mayor libertad no sea una amenaza potencial. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) se pueden configurar con un identificador de conjunto de servicio (SSID). Este SSID también debe conocerlo la tarjeta de red para poder asociarlo con el punto de acceso y así proceder con la

transmisión y recepción de datos en la red. Esto es una seguridad muy débil, si es que existe tal.

Finalmente el ultimo capitulo muestra otro aspecto muy importante de la administración de sistemas en un entorno de red puesto que se debe proteger al sistema y a sus usuarios, de intrusos. Los sistemas que son administrados descuidadamente ofrecen muchos huecos a los malintencionados: los ataques van desde averiguar las claves hasta acceder a nivel de Ethernet, y el daño causado puede ser desde mensajes de correo falsos hasta pérdida de datos o violación de la privacidad de los usuarios. Mencionaremos algunos problemas concretos cuando discutamos el contexto en el que pueden ocurrir, y algunas defensas comunes contra ellos.

Ademas se comentarán algunos ejemplos y técnicas básicas para poder lidiar con la seguridad del sistema. Por supuesto, los temas relatados aquí no pueden tratar exhaustivamente todos los aspectos de seguridad con los que uno se puede encontrar; sirven meramente para ilustrar los problemas que pueden surgir.

Otra aspecto de seguridad a considerar deberían ser aquellos programas que permiten registrarse en el sistema, o la ejecución de órdenes con autentificación limitada
La seguridad del sistema comienza con una buena administración del mismo. Esto incluye comprobar la propiedad y permisos de todos los ficheros y directorios vitales, monitorizar el uso de cuentas privilegiadas, etc.

En el presente nos introduciremos en la seguridad informática aplicada a la privacidad de nuestra información y a la protección de nuestro sistema. Para ello incluimos explicaciones de cada tema, ejemplos que ayuden a una mayor comprensión y aplicaciones que nos provean la suficiente seguridad en cuanto al uso de la red para transferir información vía inalámbrica.

Capìtulo 1 Redes de comunicación

1.1 Historia de las Redes Locales

El arte de la comunicación es tan antiguo como la humanidad. En la antigüedad se usaban tambores y humo para transmitir información entre localidades. A medida que pasó el tiempo se crearon otras técnicas como es el caso de los semáforos.

La era de la comunicación electrónica se inicio en 1834 con el invento del telégrafo, y su código asociado, el cual debemos a Samuel Morse. El código Morse utilizaba un número variable de elementos (puntos y rayas) con el objeto de definir cada carácter. El invento del telégrafo adelantó la posibilidad de comunicación humana pero, tenía muchas limitaciones. Uno de los principales defectos fue la incapacidad de automatizar la transmisión. Debido a la incapacidad técnica de sincronizar unidades de envío y recepción automática y a la incapacidad propia del código Morse de apoyar la automatización, el uso de la telegrafía estuvo limitado a claves manuales hasta los primeros años del siglo XX.

Posteriormente Emil Baudot, en Francia ideó un código en el cual el número de elementos (bits) en una señal era el mismo para cada carácter y la duración (sincronización) de cada elemento era constante. Ese código fue llamado de longitud constante.

Los trabajos sobre el problema de la sincronización comenzaron en 1869 con el desarrollo de la máquina de escribir de teclado teleimpresor en Europa. Este equipo operaba sincrónicamente; es decir, cada carácter tenía sus propios comandos *start/stop*, al comienzo y al final de cada grupo del código.

En 1876 se observa que cambios en las ondas de sonido al ser transmitidas, causan que granos de carbón cambien la resistividad, cambiando por consiguiente la corriente. En 1877 se instala la primera línea telefónica entre Boston y Sommerville, Mass.

Para 1910, un americano llamado Howard Krum introdujo mejoras en este incipiente concepto de sincronización y lo aplicó al código de longitud constante de Baudot. Este desarrollo, llamado sincronización *start/stop*, condujo a la rápida difusión del uso de equipos automáticos de telegrafía.

En 1928 las teleimpresores habían sido completamente mecanizadas: incorporaban un lector y un perforador de cinta de papel accionado por teclado; transmitían directamente por medio del teclado o por medio de la cinta y el producto final era cinta perforada o bien, copia impresa.

Esta clase de equipo teleimpresor mecánico originalmente empleaba el código de 5 niveles de Baudot y operaba a velocidades de 45 a 75 bits por segundo. Más tarde se introdujeron versiones del código ASCCI de 8 niveles que operaban a 110 bps. Incluso hasta 1970 se instalaron en todo el mundo mayor cantidad de dispositivos que

empleaban el código de Baudot, de 100 años de antigüedad, que dispositivos que empleaban cualquier otro código.

A medida que las comunicaciones se volvieron más sofisticadas, en el comienzo de los años 50 se introdujeron dispositivos electromecánicos centrales para realizar tareas como invitación (notificando en secuencia a cada estación del mismo circuito para transmitir su tráfico) y selección (notificando a una determinada estación que debe recibir un mensaje).

Paralelamente al desarrollo del telégrafo tuvo lugar el desarrollo del teléfono. El primer teléfono para uso comercial se instaló en 1877. Este sistema tenía un tablero manual. Permitía la comunicación por medio de la voz y el telégrafo a través de la misma línea, valiéndose de comunicación alternada. Alrededor de 1908, los sistemas de discado se habían difundido por casi la totalidad de EE.UU. Así, en 1920 se habían establecido los principios básicos de telecomunicaciones, conmutación de mensajes y control de línea. Los sistemas se construyeron con base en comunicación a través de la voz y transmisión (ST/SP) de caracteres de datos.

Posterior a la Segunda Guerra Mundial comenzó el desarrollo comercial de la computadora. En virtud de que estas primeras máquinas eran orientadas a lotes, no existía la necesidad de interconectarse con el sistema de comunicación que abarcaba toda la nación. Sin embargo más adelante la industria tomó conciencia de la conveniencia de que máquinas y gente hablaran entre sí. Dado que el único sistema de comunicación disponible era el telefónico, naturalmente, las computadoras en evolución, debían desarrollarse siguiendo vías que les permitieran usar este servicio.

El crecimiento del uso de la comunicación fue simultáneo al crecimiento de la tecnología de las computadoras y en parte, favorecido por él. Las redes de conmutación de mensajes, reservación y transacciones financieras de los años 50 y 60 usaban computadoras centralizadas comparativamente sofisticadas para controlar grandes poblaciones de dispositivos y terminales primitivas.

A medida que dichas redes crecían en lo que se refiere a volúmenes de tráfico y poblaciones de terminales, el aspecto no controlado de la operación de las terminales se volvió inaceptable. Luego de muchos estudios, los arquitectos del sistema finalmente determinaron que las terminales destinadas a la operación de redes basadas en computadoras debían permitir un grado de control más depurado que el alcanzado por los primeros métodos basados en electromecánica.

Razón por la cual es necesario conocer los antecedentes históricos.

1.2 Definiciones.

Las principales definiciones para efectos de este capítulo se tomaron de la Ley Federal de telecomunicaciones (Ley Federal de Telecomunicaciones, disposiciones generales, cap. 1 art. 3, fracción I), la cuál es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones y de la comunicación vía satélite.

En el artículo 3º, dicha ley proporciona las siguientes definiciones:

Telecomm: telecomunicaciones de México, Organismo Descentralizado de la Administración Pública Federal.

Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

Sistema de comunicación vía satélite: el que permite el envió de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envía de regreso a la Tierra para ser aceptadas por estación receptora.

Ondas radioeléctricas: son ondas electromagnéticas, cuyas frecuencias se fijan convencionalmente por debajo de 300GHz, que se propagan por el espacio sin guía artificial.

Enlace: medio de transmisión con características especificas, entre dos puntos, esto puede ser mediante canal o circuito (conjunto de instalaciones terminales) y red de interconexión la cual funciona en un modo particular a fin de permitir el intercambio de información entre equipos terminales.

Conmutación: proceso consistente en la interconexión de unidades funcionales, canales de transmisión o circuitos de telecomunicación por el tiempo necesario para conducir señales.

En materia de términos sobre redes de comunicación el mencionado artículo dice en sus fracciones:

VIII. *Red de telecomunicaciones*: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.
IX. *Red privada de telecomunicaciones*: la red de telecomunicaciones destinada a satisfacer necesidades especificas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red.

X. *Red pública de telecomunicaciones*: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los

equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal.

XI. *Red Local Complementaria de Telecomunicaciones*: red destinada a satisfacer necesidades de conducción de señales para grupos restringidos de usuarios, con o sin interconexión, a una red pública de telecomunicaciones. Estas redes pueden incluir, redes complementarias para fraccionamientos residenciales, parques industriales, zonas hoteleras y centros comerciales.

Punto de Conexión Terminal: Punto físico o virtual donde se conectan a una red pública de telecomunicaciones las instalaciones y equipos de los usuarios finales o, en su caso, el punto donde se conectan a éstas otras redes de telecomunicaciones.

Punto Interno de Servicio: punto dentro de una red pública de telecomunicaciones en el cual las señales son dirigidas o recibidas por el propio operador de la red pública.

Equipo Terminal de Telecomunicaciones: comprende todo el equipo de telecomunicaciones de los usuarios que se conecte más allá del punto de conexión terminal de una red pública con el propósito de tener acceso a uno o más servicios de telecomunicaciones.

Línea Telefónica: es aquel enlace con capacidad básica para transmitir principalmente señales de voz, entre un centro de conmutación público y un punto de conexión terminal una caseta pública telefónica una instalación telefónica privada o cualquier otro tipo terminal que utilice señales compatibles con la red pública telefónica.

Red Pública Telefónica: Red Pública de Telecomunicaciones cuyos concesionarios deben prestar el servicio público de telefonía básica.

Red Pública Telegráfica: Red Pública de Telecomunicaciones por medio de la cual se presta el servicio público de telégrafos y giros telegráficos y radiotelegrafía dentro del territorio nacional con interconexión a otras redes del extranjero.

Red Local: red de telecomunicaciones que permite la comunicación dentro del área de servicio local autorizada y en su caso la interconexión de acceso a redes para servicios de larga distancia.

Red de Larga Distancia: red de telecomunicación que permite la comunicación de larga distancia nacional e internacional entre usuarios localizados en distintas áreas de servicio local utilizando en su caso la interconexión con las diferentes redes locales". [*Ley general de disposiciones generales*]

Canal: es un medio de transmisión unidireccional de señales entre dos puntos, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

Circuito: combinación de dos canales que permite la transmisión bidireccional de señales entre dos puntos. En una red de telecomunicaciones el término circuito esta limitado generalmente a un circuito de telecomunicaciones que conecta directamente dos equipos o centrales de computación, junto con los equipos terminales asociados.

III.- En materia de redes y estaciones de radiocomunicación.

Red de Radiocomunicación es aquella integrada por una o varias estaciones radioeléctricas, incluyendo en su caso, los equipos de conmutación y enlaces radioeléctricos asociados así como la asignación de frecuencias necesarias para establecer los servicios de radiocomunicación;

Sistema o Red Celular de Radiocomunicación: sistema o red de radiocomunicación para servicio móvil en tierra de alta capacidad en el cual el espectro de frecuencia asignado se divide en canales discretos los cuales a su vez son asignados en grupos de células geográficas para cubrir un área geográfica de servicio celular. Los canales discretos son susceptibles de ser reutilizados en diferentes células dentro del área de servicio.

Estación o Estación Radioeléctrica: consiste en uno o más equipos transmisores o receptores o una combinación de éstos incluyendo las instalaciones accesorias necesarias para asegurar un servicio de radiocomunicación o de radioastronomía en un lugar determinado.

Las estaciones se clasificarán según el servicio en el que participen de una manera permanente o temporal.

Estación Terrenal: estación situada en la superficie de la tierra para efectuar radiocomunicaciones terrenales". Toda estación que se mencione en el presente Reglamento, salvo indicación expresa "corresponderá a una estación terrenal.

Estación fija: estación de servicio fijo.

Estación móvil: estación de servicio móvil destinada a ser utilizada en movimiento o mientras esté detenida en puntos no determinados.

Estación terrestre: estación de servicio móvil no destinada a ser utilizada en movimiento.

Estación Base: estación terrestre para proporcionar el Servicio móvil terrestre.

Estación Terminal de Radiocomunicación: uno o más transmisores o receptores o combinación de ambos incluyendo las instalaciones accesorias mediante el cual un usuario o suscriptor establece el enlace radioeléctrico en el punto de conexión terminal virtual, con el propósito de tener acceso a uno o más servicios de radiocomunicación.

Estación Experimental: estación que utiliza las ondas radioeléctricas para efectuar experimentos que pueden contribuir al progreso de la ciencia o de la técnica.

IV.- En materia de redes, sistemas y estaciones de comunicación por satélite.

Red de Comunicación por Satélite: es la que se integra por un sistema de satélites o parte del sistema, y las estaciones terrenas asociadas, con la asignación de frecuencias necesarias para establecer los servicios de comunicación por satélite.

Sistema de satélites de comunicación: sistema de satélites artificiales de la tierra colocados en órbita en el espacio con el propósito de establecer radiocomunicación entre estaciones terrenas. El sistema comprende a su vez las estaciones terrenas con los equipos e instalaciones necesarias para el monitoreo y control de los satélites.

Sistema de satélites nacionales: sistema de satélites establecido para satisfacer necesidades nacionales de radiocomunicación por satélite.

V.- En materia de Servicios de Telecomunicaciones la Ley Federal de Telecomunicaciones y disposiciones generales en su capítulo V establece las siguientes definiciones.

Servicios de Telecomunicaciones: son aquellos que se ofrecen a terceros o al público en general, para que por medio de un circuito o una red de telecomunicaciones un usuario pueda establecer comunicación desde un punto de la red a cualquier otro punto de la misma o a otras redes de telecomunicaciones.

Prestadores de Servicios de Telecomunicaciones: personas físicas o morales que prestan servicios de telecomunicaciones y cuentan para ello con una concesión para instalar, operar y explotar una red de telecomunicaciones o cuentan con un permiso para prestar servicios de telecomunicaciones utilizando las redes concesionadas a otros.

Operador de Red Pública de Telecomunicaciones: persona física o moral que cuenta con una concesión para prestar servicios públicos de telecomunicaciones mediante la instalación, operación y explotación de una red pública de telecomunicaciones, incluyendo los organismos descentralizados del Gobierno Federal que operan redes públicas de telecomunicaciones.

Servicio Privado de Telecomunicaciones: el establecido para satisfacer necesidades de comunicaciones internas o privadas de una persona física o moral a través de una red privada.

Servicios Básicos de Telecomunicaciones: son servicios de carácter estratégico para el desarrollo nacional, que comprenden además de los servicios públicos de telefonía básica, telégrafos y comunicación nacional por satélite, la instalación, establecida, operación y explotación de redes públicas de telecomunicaciones en el territorio nacional.

Servicios de Telecomunicaciones de Valor Agregado: son los servicios que se prestan a terceros, utilizando como soporte para la conducción de señales una red pública de telecomunicaciones o privadas o complementarias locales.

Servicio Público de Telefonía Básica: servicio final de telecomunicaciones por medio del cual se proporciona la capacidad completa para la comunicación de voz entre usuarios, incluida la conducción de señales entre puntos terminales de conexión, así como el cableado y el primer aparato telefónico terminal, a solicitud del suscriptor. Dicha conducción de señales constituye la que se proporciona al público en general, mediante la contratación de líneas de acceso a la red pública telefónica, que utilizan las centrales públicas de conmutación telefónica, de tal manera que el suscriptor disponga de la capacidad para conducir señales de voz de su punto de conexión terminal a cualquier otro punto de la red pública telefónica, de acuerdo a una renta y tarifa que varía en función del tráfico que se curse.

Servicio de Interconexión a Redes Públicas: es el servicio de conducción de señales que presta un concesionario, por medio de su red pública de telecomunicaciones, a otras empresas de telecomunicación, para combinar o complementar sus propias instalaciones con el objeto de proporcionar un servicio final.

Servicio de Comunicación de Datos: consiste en la transferencia de información entre unidades funcionales mediante transmisión de datos conforme a un protocolo.

Interferencia Admisible: interferencia observada o prevista que satisface los criterios cuantitativos de interferencia y de compartición que figuran en las normas técnicas establecidas por la Secretaría, o en el Reglamento de Radiocomunicaciones de la Unión Internacional de telecomunicaciones, o en recomendaciones del Comité Consultivo.

Interferencia Perjudicial: interferencia que compromete el funcionamiento de un servicio de radionavegación o de otros servicios de seguridad o que degrada gravemente, interrumpe repetidamente o impide el funcionamiento de un Servicio de radiocomunicación explotado de acuerdo con el presente Reglamento.

Zona de Coordinación: zona asociada a una estación terrena fuera de la cual una estación terrenal, que comparte la misma banda de frecuencias, no puede producir ni sufrir ninguna interferencia superior a la interferencia admisible.

El reglamento en estudio remite a el Convenio Internacional de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), por sus reglamentos vigentes y por las definiciones que en su caso emitan los Comités Consultivos Internacionales Telefónico y Telegráfico y de Radiocomunicaciones (CCITT y CCIR). (Ley Federal de Telecomunicaciones, disposiciones generales, cap. 1 art. 3, fracción I ,II, VII, IX, X, XI,. XII, XIV.)

1.3 Protocolos

En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de

comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

Como se mencionó anteriormente, OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.
Estos equipos presentan diferencias en:
1. Procesador central
2.Velocidad
3.Memoria
4.Dispositivos de almacenamiento
5.Interfaces para comunicaciones
6.Códigos de caracteres
7.Sistemas operativos

Estas diferencias propician que el problema de comunicación entre computadoras no tenga una solución simple.

Dividiendo el problema general de la comunicación, en problemas específicos, facilitamos la obtención de una solución a dicho problema.

Esta estrategia establece dos importantes beneficios:

A) Mayor comprensión del problema.

B)La solución de cada problema especifico puede ser optimizada individualmente.

Este modelo persigue un objetivo claro y bien definido: formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independientemente del:
I· Fabricante.
II· Arquitectura.
III· Localización.
IV· Sistema Operativo.

Alcanzar este objetivo tiene las siguientes implicaciones:

1. Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APLICACIÓN.

2. Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones especificas diseñadas para atender el protocolo de la capa superior.

4. Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada capa.

El objetivo perseguido por la estructura del Modelo OSI es establecer una estructura que presenta las siguientes particularidades:

a) Estructura multinivel: la cual se diseñó con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones especificas.

b) El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora.

La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

c) Puntos de acceso: entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

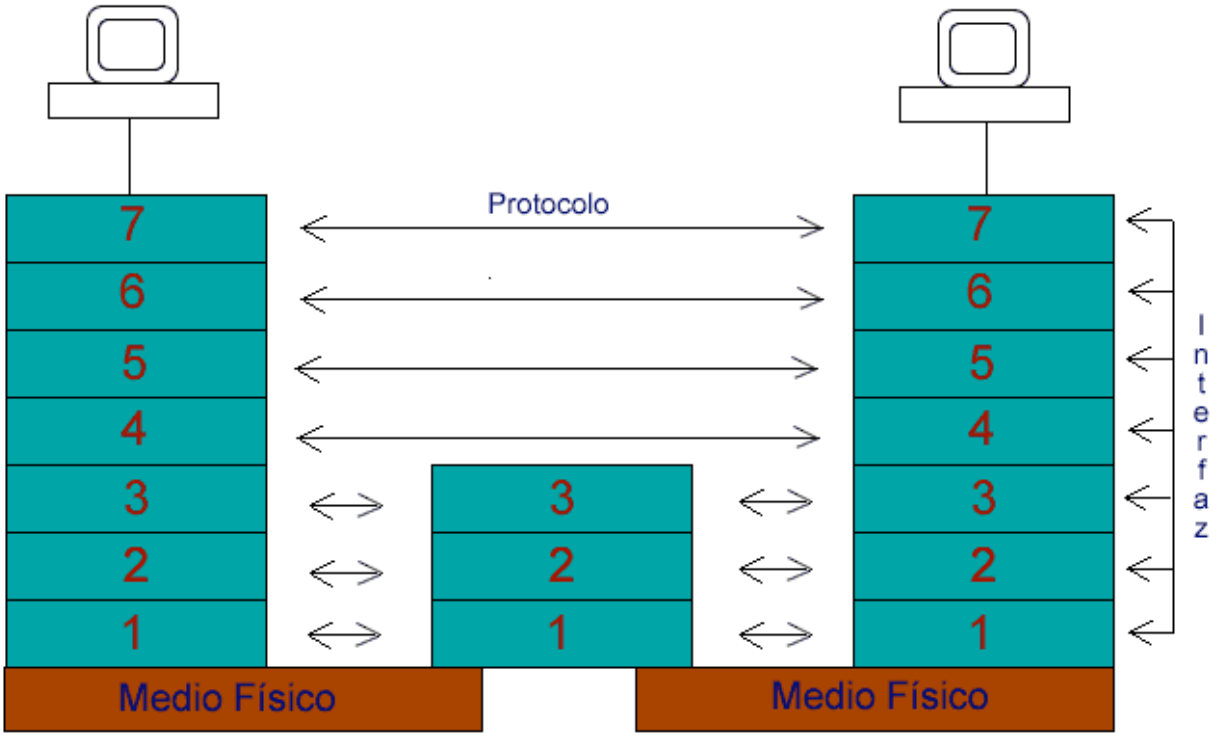
d) Dependencias de niveles: cada nivel es dependiente del nivel inferior y también del superior.

e) Encabezados: en cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: encabezado e Información. Entonces, la incorporación de encabezados es necesaria, aunque representa información extra, lo cual implica que un mensaje corto pueda ser voluminoso.
Sin embargo, la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

Unidades de información: En cada nivel, la unidad de información tiene diferente nombre y estructura :

Niveles del Modelo OSI.

A)Aplicación.
B)Presentación.
C)Sesión.
D)Transporte.
E)Red.
F)Enlace de datos.
G)Físico.



Elaborado por: "Aguirre José E. (2000).Redes Inalámbricas. URL; http://wwww.lafacu.com/apuntes/informatica/redes_inalamb/default.htm"

La descripción de los 7 niveles es la siguiente :

El primer Nivel Físico: Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

I. Definir conexiones físicas entre computadoras.
II. Describir el aspecto mecánico de la interface física.
III. Detallar el aspecto eléctrico de la interface física.
IV. Escribir el aspecto funcional de la interface física.
V. Definir la técnica de transmisión.
VI. Dar el tipo de transmisión.
VII. Proporcionar la codificación de línea.
VIII. Definir la velocidad de transmisión.
IX. Definir el modo de operación de la línea de datos.
("Black Uyless. Redes de computadores, 1997, p. 162")

Segundo Nivel Enlace de Datos: este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

- Detectar errores en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.

- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.

En general controla el nivel y es la interface con el nivel de red, al comunicarle a este una transmisión libre de errores.

Tercer Nivel de Red: este nivel define el enrutamiento y el envío de paquetes entre redes.

- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

Cuarto Nivel de Transporte: este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento. Además, garantiza una entrega confiable de la información.

- Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).
- Este nivel define como direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Describe la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos, e incluye la confiabilidad en la transferencia de información entre dos sistemas.

Quinto Nivel Sesión: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

Sexto Nivel Presentación: traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.

- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Realiza la visualización.

Séptimo Nivel Aplicación: Proporciona servicios al usuario del modelo OSI.

- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones especificas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

1.4 Topologías de Redes Locales

Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman. Los Criterios a la hora de elegir una topología, en general, buscan que eviten el coste del encaminamiento (necesidad de elegir los caminos más simples entre el nodo y los demás), dejando en segundo plano factores como la renta mínima, el coste mínimo, etc. Otro criterio determinante es la tolerancia a fallos o facilidad de localización de éstos.

La forma como se construye la red que soporte la comunicación entre los dispositivos de comunicación de datos esta representada por la topología de la red local.

Las topologías comúnmente usadas en la construcción de redes de área local son:

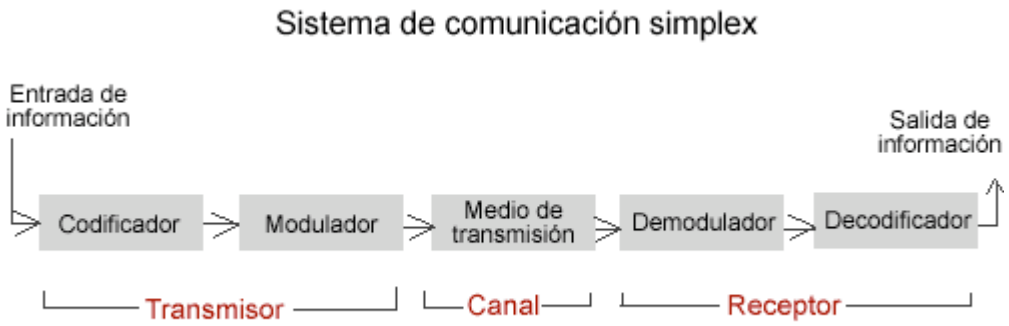
1. Topología de Anillo
2. Topología de Bus
3. Topología de Árbol
4. Topología de Estrella

1.4.1 Topología de Anillo.

En esta topología la red consiste en un conjunto de repetidores unidos por líneas de comunicación punto a punto, que forman un ciclo cerrado.

Cada repetidor participa en dos enlaces, recibe datos de uno y los transmite al otro; su capacidad de almacenamiento, si tiene, es de sólo unos cuantos bits y la velocidad de recepción y de transmisión es igual en todos los repetidores.

Los enlaces (líneas de comunicación) son simplex, por lo tanto la información fluye en un solo sentido en el anillo. Las estaciones se conectan a la red por medio de los repetidores.

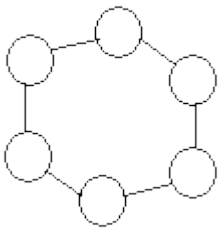


Elaborado por**: "** Grupo Penteo (2001) ¿Qué son las redes inalámbricas?, URL; **http://www.expansionyempleo.com/edicion/noticia/0,2458,41089,00.html** "

Una red con topología de anillo se organiza conectando nodos de la red en un ciclo cerrado con cada nodo enlazado a los nodos contiguos a la derecha y a la izquierda. La ventaja de esta red es que se puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.

Algunas veces, estas redes utilizan esquemas de transmisión de señales para determinar que nodo puede tener acceso al sistema de comunicaciones.

Elaboración propia
fig. 1.4.1 .

Anillo	
Los nodos de la red están conectados unos con otros en la forma de un anillo. Así, cada nodo está conectado a dos más en la red. **Pros:** - Mejora en el ancho de banda **Contras:** - El anillo tiene que estar cerrado; si cae un nodo, toda la red falla.	

Elaboración propia.

1.4.2 Topología de Bus

En esta topología, las estaciones comparten una misma línea de comunicación (medio). Cuando una estación quiere transmitir, simplemente envía sus tramas al bus (medio de comunicación).

Cuando una señal atraviesa el bus (normalmente un cable coaxial), todas y cada una de las estaciones escuchan la señal que lleva consigo una designación de dirección.

Los sistemas de bus, como Ethernet o la mayoría de los sistemas de banda ancha, emplean un cable bidireccional con trayectorias de avance y regreso sobre el mismo medio, o bien emplean un sistema de cable doble o dual para lograr la bidireccionalidad.

Aquí no existe un nodo central, si no que todos los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro.

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en un disposición en estrella. Pero, por contra, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

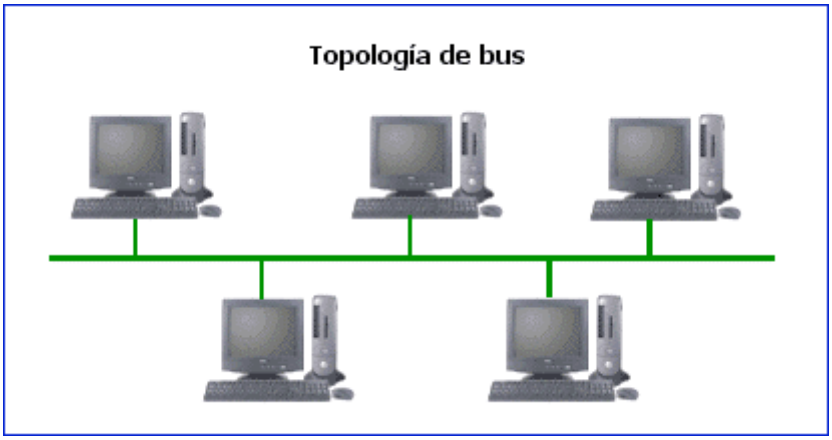
Debido a que en el bus la información recorre todo el bus bidireccionalmente hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en una Red en estrella debido a la modularidad que ésta posee.

La red en bus posee un retardo en la propagación de la información mínimo, debido a que los nodos de la red no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Esta pasividad de los nodos es debida mas bien al método de acceso empleado que a la propia disposición geográfica de los puestos de red.

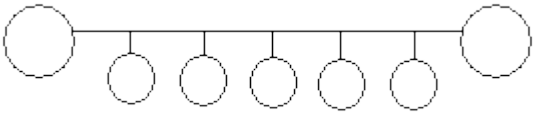
La Red en Bus necesita incluir en ambos extremos del bus, unos dispositivos llamados terminadores, los cuales evitan los posibles rebotes de la señal, introduciendo una impedancia característica (50 Ohm.)

Añadir nuevos puesto a una red en bus, supone detener al menos por tramos, la actividad de la red. Sin embargo es un proceso rápido y sencillo.

Es la topología tradicionalmente usada en redes Ethernet.



Elaboración propia.
fig. 1.4.2

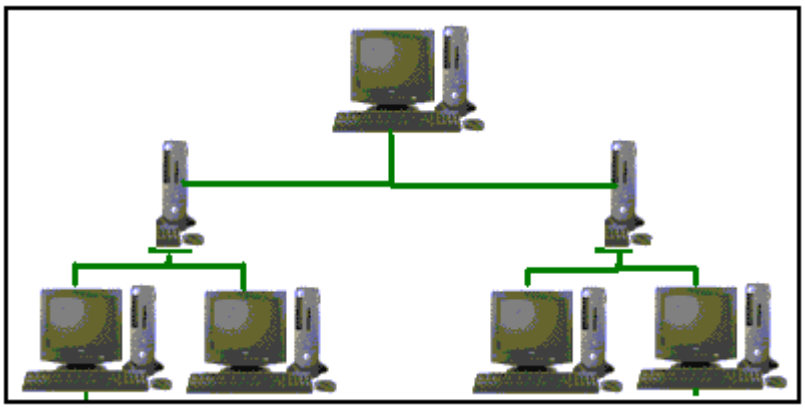
Bus Todos los nodos en la red están conectados a un cable central llamado 'backbone'. **Pros:** - Fácil de implementar **Contras:** - Punto de falla en el cable central; si cae un nodo, toda la red falla.	

Elaboración propia.

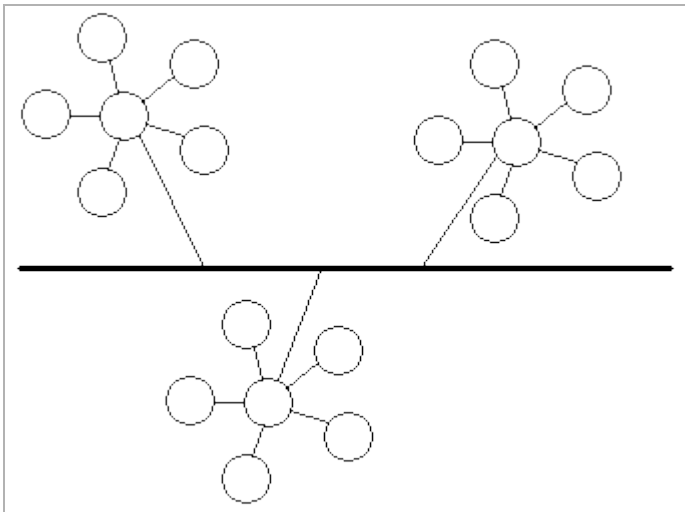
1.4.3 Topología de Árbol

La topología en árbol es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz . Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.



Elaboración propia
fig. 1.4.3

Árbol	
Topología híbrida que agrupa redes en forma estrella y las conecta a un bus central o 'backbone' **Pros:** - Seguridad con velocidad - El backbone puede ser de alta velocidad **Contras:** - Punto de falla en el cable central; si cae un nodo, toda la red falla.	

Elaboración propia.

1.4.4 Topología de Estrella

En la topología en estrella, cada estación tiene una conexión directa a un acoplador (conmutador) central. Una manera de construir esta topología es con conmutadores telefónicos que usan la técnica de conmutación de circuitos.

Otra forma de esta topología es una estación que tiene dos conexiones directas al acoplador de la estrella (nodo central), una de entrada y otra de salida (la cual lógicamente opera como un bus). Cuando una transmisión llega al nodo central, este la retransmite por todas las líneas de salida.

Según su función, los acopladores se clasifican por su función en:

A) Acoplador pasivo: cualquier transmisión en una línea de entrada al acoplador es físicamente trasladada a todas las líneas de salida.

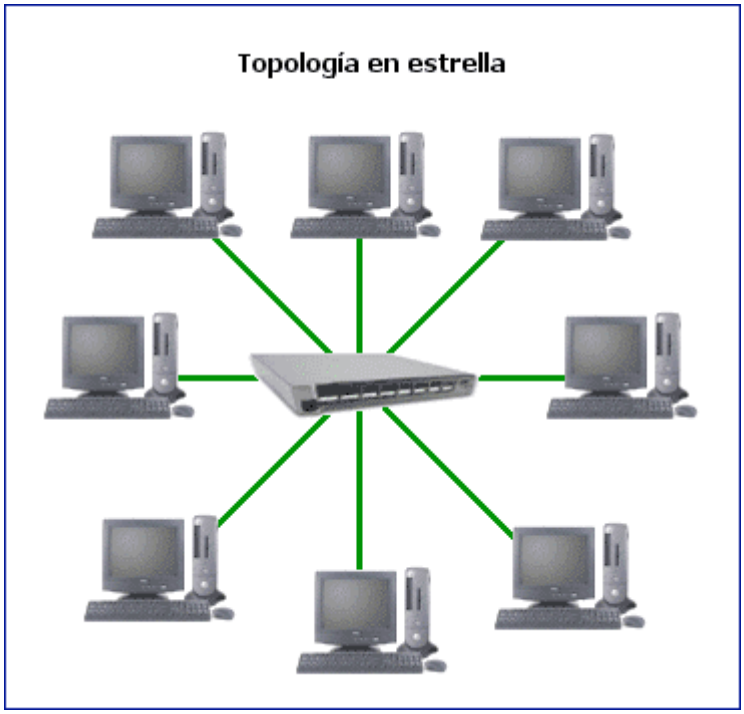
B) Acoplador activo: existe una lógica digital en el acoplador que lo hace actuar como repetidor. Si llegan bits en cualquier línea de entrada, son automáticamente regenerados y repetidos en todas las líneas de salida. Si llegan simultáneamente varias señales de entrada, una señal de colisión es transmitida en todas las líneas de salida.

Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los radios de una rueda.

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la *gran seguridad* que suele poseer dicho nodo. Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.

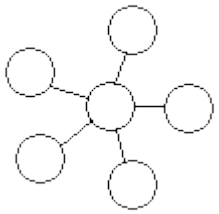
Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

La topología en estrella es empleada en redes Ethernet y ArcNet.



Elaboración propia.

fig. 1.4.4

Estrella	
Todos los nodos están conectados a un concentrador central. Los nodos se comunican entre sí pasando por el concentrador, quien dirige el tráfico de la red. **Pros:** - Bastante segura **Contras:** - Punto de falla en el concentrador	

Elaboración propia.

Diferentes formas de topología y la longitud máxima de los segmentos de cada una

TOPOLOGÍA DE RED	LONGITUD SEGMENTO MÁXIMO
Ethernet de cable fino **(BUS)**	185 Mts (607 pies)
Ethernet de par trenzado **(Estrella/BUS)**	100 Mts (607 pies)
Token Ring de par trenzado **(Estrella/Anillo)**	100 Mts (607 pies)
ARCNET Coaxial **(Estrella)**	609 Mts (2000 pies)
ARCNET Coaxial **(BUS)**	305 Mts (1000 pies)
ARCNET de par trenzado **(Estrella)**	122 Mts (400 pies)
ARCNET de par trenzado **(BUS)**	122 Mts (400 pies)

1.5 Protocolos de Comunicación

Los principales parámetros que caracterizan a los protocolos de acceso al medio son: el dónde y el cómo se lleva a cabo el control.

Los protocolos que han tenido mayor aceptación son aquellos que realizan el control de una forma distribuida.

El Round Robin es el que se da a cada estación bajo un determinado orden una oportunidad para transmitir.

Token Bus: Estandarizado por el IEEE 802.4. Es un protocolo "round robin" distribuido. En los ultimos años se han propuesto una serie de protocolos de acceso al medio para la topología en anillo.

Token Ring es un protocolo "round robin" distribuido.

El protocolo que se utilice para controlar el acceso al medio en gran parte define el desempeño de una red local.

El desempeño de una red local con un protocolo de acceso al medio ideal, es uno de los parámetros más utilizados para medir la eficiencia de una red local son:

1) El tiempo promedio de atraso desde que el paquete está listo para la transmisión hasta que se ha transmitido exitosamente.
2) El flujo en la red (throughput).
3) La utilización del medio de comunicación.

Para comprender cómo influye el tiempo de propagación de la información a través del medio en el rendimiento de la transmisión (velocidad de transmisión), es necesario comprender primero que:

A) Razón de transmisión (velocidad de transmisión) en bits/segundo.
B) Longitud del medio de comunicación.
C)Velocidad de la onda electromagnética en el medio de transmisión.
D) Longitud de los paquetes de datos en bits.

Métodos de acceso: “un método de acceso es una técnica de control de acceso al medio que establece las reglas que indican como un nodo de red puede hacer uso del medio de comunicación para transmitir su información. Es en si programación que apoyada en hardware determina en que momento y cómo, un nodo de red accesa al medio. Esto es, el método de acceso provee el control lógico del medio físico del que se dispone para la comunicación. “[Black, 1997]

CSMA/CD.

Este método de acceso tiene como objeto proveer accesos múltiples a los nodos de una red con topología de bus, y está basado en el principio de sensar el medio de comunicación antes y durante la transmisión de un paquete de información, asumiendo que el retraso en la propagación es muy corto comparado con el tiempo de transmisión del paquete de datos. (“Black Uyless. Redes de computadores, protocolos, normas e interfaces, , 1997, pag. 165”)

CSMA/CD proviene de las siglas en inglés de Carrier Sense Multiple Access with Colision Detection. Esta técnica de acceso al medio (MAC) es una de las más utilizadas en topologías bus\árbol. Originalmente fue desarrrollada por Xerox para su red local Ethernet. El comité de la IEEE 802 creó el estándar IEEE 802.3 basado en esta técnica de acceso al medio para banda base. Esta técnica es una evolución de las técnicas de acceso aleatorio Aloha. En un canal Aloha puro, las terminales transmiten cuando lo necesitan, sin importar si hay una trasmisión en progreso. El control de acceso al medio es muy sencillo pero la máxima utilización es solamente del 18%.

Posteriormente se desarrolló el canal Aloha sincronizado (Sloteed Aloha), en el cual las terminales solamente pueden iniciar transmisiones al inicio de una ranura de t segundos, donde t es el tiempo de transmisión de un paquete (longitud fija). Con esto se logra una utilización máxima del 36%.

Tratando de incrementar la utilización de los canales de comunicación, se creó la técnica CSMA (Carrier Sense Multiple Access). La idea básica del CSMA es que cuando una terminal necesita transmitir, primero revisa al medio de transmisión para ver si no hay una transmisión en progreso y evitar así una colisión. Si el medio está libre, transmite; si está ocupado, espera.

1) Está modificación, aún cuando parece simple y obvia, logra incrementar la utilización de los canales Aloha, ya que reduce el intervalo de colisión y, por lo tanto, reduce el número promedio de colisiones, pero no las evita, ya que dos o más terminales pueden iniciar una transmisión al mismo tiempo y producir una colisión. En los canales Aloha se utilizaba transmisión por señales de radio con una velocidad de transmisión relativamente baja y el tiempo de transmisión resultaba mucho mayor que el tiempo de propagación de la señal de radio desde la estación transmisora hasta la estación central receptora. (“Aguirre José E. (2000).Redes Inalámbricas. URL; http://wwww.lafacu.com/apuntes/informatica/redes_inalamb/default.htm”)

En redes locales esto no sucede por dos razones:

1) La velocidad de la onda electromagnética en medios guiados es 2/3 de la velocidad en el aire.
2) Las velocidades de transmisión son mucho mayores que las utilizadas originalmente en canales Aloha.

Por ejemplo, se considera una red Ethernet 10Base5 con 5 segmentos. (10Base5 significa velocidad = a 10 Mbps, transmisión banda base y longitud máxima de cada segmento = 500 metros).

La velocidad de propagación es 2x10^8 y la longitud de la red es de 2500 metros, lo cual da un tiempo de propagación de 12.5 ms, esto sin considerar atrasos en repetidores entre segmentos.

La velocidad de transmisión es de 10 Mbps y suponiendo paquetes de 512 bits, da un tiempo de transmisión de 51.2 ms.

Como puede verse, los puntos ahora son del mismo orden.

Si la terminal que esta en un extremo de la red inicia una transmisión en el tiempo t0, la terminal que está en el otro extremo no se dará cuenta antes de 12.5 ms, propiciando que esta última crea que el medio está libre e inicie una transmisión que ocasiona una colisión. La utilización máxima usando CSMA depende de la relación del tiempo de propagación con el tiempo de transmisión. En redes locales está relación se conoce como "a".

Los valores de la "a" pequeños favorecen una utilización mayor de la red, mientras que los valores grandes provocan una utilización menor.

El tiempo que se desperdicia en terminar de transmitir los paquetes cuando hay colisión no tiene sentido. Esto dió origen a la técnica de acceso al medio CSMA\ CD (Carrier Sense Multiple Access with Collison Detection).

El protocolo CSMA\CD añade las siguientes reglas a CSMA:

1. Si se detecta una colisión durante la transmisión, se suspende la transmisión del paquete inmediatamente y se genera una señal breve que indica que hubo colisión (jamming signal).

2. “Después de indicar la colisión, se genera un tiempo aleatorio, transcurrido este, se intenta llevar a cabo la transmisión usando CSMA”. [Black Uyless, 1997]

Al ver las redes estás entran de acuerdo a el área en la que se pretendan que van he estar así como por las distancias y usuarios que harán uso de la misma.

De acuerdo a todos estas consideraciones se catalogan de la siguiente forma:

LAN : es una red de área local para una sola ubicación física en donde se encuentran incluidos todos los dispositivos.

WAN: es una red de área amplia consiste básicamente en la unión de 2 ó más redes LAN.

MAN: es una red de área Metropolitana concepto base que el de WAN.

Con él pasó del tiempo el avance tecnológico del mundo la necesidad de una red LAN a crecido considerablemente así como él consumó y uso de las redes tradicionales de cobre se ha estado y se volverá más grande cada vez.

Dentro de este tipo de redes se pueden construir muy independientemente de cualquier circunstancia, siempre se deverá de llevar a cabo al pie las consideraciones técnicas y reglamentaciones para su correcta funcionalidad y óptimo desempeño.

Así como para su construcción se podrán utilizar diferentes elementos ya sean pasivos o activos para mantener siempre en standar la implementación y operatividad de la red.

¿Cuándo se sugiere utilizar una red LAN?

Cuando las aplicaciones que se vayan a utilizar sean consideradas de uso compartido o común así cuando haya la necesidad de intercambiar información, utilizar recursos compartidos y bajar costos de operación por no contar con medios de propagación de archivos y formatos de vídeos, gráficas, bases de datos y todos los demás elementos que ponen en sobre utilización a la Red.

Con él tiempo y el aumento y necesidad de interconectar varios lugar físicos por medio de conexiones denominados enlaces WAN, la necesidad de una red WAN a crecido considerablemente así como él consumó y uso de las redes tradicionales de cobre se ha estado y se volverá más grande cada vez.
WAN red de área amplia consiste básicamente en la unión de 2 ó más redes LAN.

Dentro de este tipo de redes se pueden construir muy independientemente de cualquier circunstancia, siempre se deberá de llevar a cabo al pie las consideraciones técnicas y reglamentaciones para su correcta funcionalidad y óptimo desempeño.

Así como para su construcción se podrán utilizar diferentes elementos activos para mantener siempre en estándar la implementación y operatividad de la red.

Una red WAN se sugiere utilizar cuando:

Cuando las aplicaciones que se vayan a utilizar sean consideradas de uso compartido o común así cuando haya la necesidad de intercambiar información, y esta sea necesaria que se encuentre disponible en varios puntos físicos distantes o en su momento se requiera para optimizar la operación diaria se realice él envió y recepción de información en línea con los puntos distantes.

Una WAN constituye un sistema de comunicación que interconecta sistemas de computadoras geográficamente remotos. Enlaza las computadoras situadas fuera de las propiedades de una organización (edificios o campus) y atraviesa áreas públicas que están reguladas por autoridades locales, nacionales e internacionales. Generalmente, el enlace entre lugares remotos se realiza a través de la red pública de teléfono, pero una organización podría crear sus propios enlaces WAN mediante satélites, microondas u otras tecnologías de comunicación. Una WAN (Wide Area Network), es una red con proporciones potencialmente globales. Si se emplean facilidades públicas, una WAN involucrará compañías de telecomunicaciones para el intercambio local (LECs, Local Exchange Carriers), para el intercambio de larga distancia (IXCs, Interexchange Carriers) y para lugares remotos.

WAN punto a punto

Una red de punto a punto es sin duda la más sencilla, ya que tiene sólo una computadora, una línea de comunicación y una terminal en el otro extremo del cable.

La terminal puede ser una terminal de lote distante (RBT) o interactiva. Esta fue la primera forma de red existente, y muchas redes conservan esta estructura, se desarrollan gradualmente en entidades más complejas. En un sistema de este tipo la computadora central no necesita ser muy grande. Una microcomputadora puede actuar como anfitriona de una o más terminales. Sin embargo, normalmente estos sistemas tienen una computadora grande como sistema anfitrión.

WAN Broadcast

El tráfico de banda ancha (broadcast) existe en todas la redes actuales y no es la excepción en las redes virtuales a de switches, debido a que no se genera por la tecnología, sino por las aplicaciones mismas que utilizan este tipo de tráfico para enviar o recibir información, por ejemplo, en la multimedia. El tráfico broadcast se controla a través de una segmentación en la red eficiente, o bien, mediante el análisis del comportamiento de las aplicaciones antes de instalarlas.

En la operación normal de la red, el tráfico broadcast puede deberse a un mal funcionamiento en algunos de los dispositivos: como las tarjetas de las estaciones de trabajo, del concentrador o bien del enrutador; o también debido, al mal estado de algún dispositivo adicional como el puente, repetidor y/o gateway. Si este tipo de tráfico no se maneja bien, puede causar serios problemas a la red e incluso puede darla de baja en su totalidad. Este tipo de falla se debe primordialmente al uso inadecuado de protecciones contra este tipo de tráfico (firewalls), a la generación de círculos en la interconectividad, a la falla de los dispositivos y/o a las aplicaciones que hacen un uso intenso de broadcast para operar.

Por lo tanto, los administradores de redes deben tomar precauciones contra este tipo de tráficos. Una forma común y muy utilizada para hacerlo es la segmentación de la red con dispositivos que no permitan la propagación del broadcast, es el caso de los enrutadores en hardware y firewalls en software. Éstos protegen a los demás segmentos dentro de la red en el caso de que alguno de ellos tengan problemas, debido a que los broadcast no serán propagados hacia los demás segmentos ocasionando fallas en la red.

Un aspecto muy importante a considerar cuando se migra a redes de switches o virtuales es que los broadcast funcionan en el nivel 2, al igual que las redes virtuales.
Si no se considera un esquema de protección contra el tráfico no deseado (broadcast), cuando ocurra un problema en la red éste será propagado hacia todos los puertos del switch y, por consiguiente, hacia toda la red, ocasionando que todas las aplicaciones dejen de funcionar. A este tipo de configuraciones se le conoce como "red plana" debido a que toda la red opera como un solo dominio de broadcast. Las ventajas de las redes planas son la reducción en el tiempo de retraso de los paquetes y el incremento en el rendimiento de la red; la desventaja es el incremento en la susceptibilidad de los problemas de broadcast a través de todos los switches, puertos, backbones y usuarios.
Al igual que los enrutadores actuales, las redes virtuales ofrecen mecanismos eficientes para el manejo de los problemas potenciales de broadcast, sin perder sus ventajas. Para poder manejar de forma controlada estos problemas, cada puerto del switch, al igual que los usuarios, se intergra a grupos de trabajo o de redes virtuales con el fin de aislarlos cuando se genere algún problema en cualquiera de ellos. El tráfico broadcast de un grupo de trabajo o VLAN no se transmite fuera de el mismo .

Con esta sencilla estrategia, los administradores de red pueden controlar fácilmente el tamaño de los grupos de trabajo o VLAN, de tal forma que el tráfico broadcast generado en esa VLAN no sea perjudicial para ella misma. Entre más pequeñas sea la VLAN, menor será el tráfico de broadcast generado.

Topologías WAN

Existen diversas formas en las que podrían organizarse las redes, y la mayoría de las redes se encuentran en un constante estado de transición y desarrollo. “Si la red de computadoras tiene sólo una ubicación central o computadora anfitriona que realiza todas las tareas de procesamiento de datos desde uno o más lugares distantes o remotos, se trata de una red centralizada”. [Caballero. 1999]

Si hay computadoras distantes procesando trabajos para usuarios finales, y también una computadora ubicada en un sitio central (es decir, opcional), entonces podemos tener los inicios de una red distribuida. Una red distribuida puede ser centralizada o dispersa; pero una red en la que no se realiza procesamiento distribuido sólo puede ser centralizada ya que todas las tareas de procesamientos de datos se efectúan en una computadora ubicada en un sitio central.

Es posible que un solo sistema de comunicaciones genere comunicaciones para dos o más redes de computadoras en operación concurrente.

Las topologías de red describen la distribución física de la red. “Una inter-red consta de LANs departamentales o de estaciones de trabajo que se interconectan con puentes o encaminadores”. En un entorno local, tal como un edificio, frecuentemente se utiliza un cable soporte, pero para construir redes de área metropolitana o extensa se utilizan los servicios públicos, como los que ofrecen las compañías telefónicas. Las tres topologías principales en las WANs son:

1. **Red soporte**

Típicamente encontrada en entornos de oficina o campus en los que los departamentos edificios se interconectan a través de los cables soportes. Los puentes o encaminadores gobiernan el flujo de tráfico entre las subredes unidas y el soporte.

2. **Red de malla**

Los encaminadores se interconectan con otros encaminadores. La topología se puede configurar localmente, pero frecuentemente se encuentra en redes de área metropolitana o extensa que conectan oficinas remotas mediante enlaces de telecomunicaciones. Se utilizan los encaminadores para elegir el trayecto mejor y más

eficiente de la fuente al destino a través de la malla. Los enlaces que fallan se evitan con el uso de otros trayectos de la malla.

3. Redes centralizadas (estrella)

"Una red centralizada es aquella en la cual las operaciones de cómputo primarias se realizan en un solo lugar, donde todas las estaciones distantes alimentan de información a la central". (" Black Uyless. Redes de computadores, protocolos, normas e interfaces, 1997 p.168") A menudo un sistema de este tipo es concebido como una red en estrella donde cada sitio remoto ingresa al sistema central vía una línea de comunicación, aunque los sistemas punto a punto y multipuntos clásicos eran también redes centralizadas.

Sin embargo, en términos generales una red multipuntos no tenía recursos de procesamiento distribuido, aunque una red en estrella puede tener otras computadoras en el otro extremo de sus líneas de comunicaciones. La computadora que soporta una red de multipuntos tradicional podría haber sido enlazada a una red en estrella. Los sistemas EPABX, basados en la tecnología telefónica, es la tecnología de redes de área local que utiliza una topología de estrella donde el conmutador o interruptor constituye el nodo central.

Capitulo 2. Redes inalámbricas

La comunicación, sería imposible sin algún tipo de lenguaje o código. En la jerga de las redes de computadoras, estos lenguajes se denominan conjuntamente como protocolos. No obstante, no se debería pensar aquí en lenguajes ya escritos y definidos, sino más bien en el código de comportamiento altamente formalizado.

Las redes inalámbricas se construyen utilizando dos topologías básicas. Estas topologías se llaman de distintas formas, incluyendo administradas y no administradas, "hosted" y de punto a punto ("peer-to-peer"), así como de infraestructura y ad-hoc. En este documento utilizaremos los términos "infraestructura" y "ad-hoc". Estos términos se relacionan esencialmente con las mismas funciones básicas de la topología.

Una topología de infraestructura amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica. El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice y el producto del proveedor. En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

“Una topología ad-hoc es una en la cual se crea una red LAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso” (“Buet Santana, Vicente (1998). Redes inalámbricas de área local. URL; http://wwwtimagazine.net/magazine/0798/wireles.cfm”). Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar ideas, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

Cuando se combinan la nueva generación de software y las soluciones inteligentes de punto a punto, estas redes inalámbricas ad-hoc pueden permitir a los usuarios que viajan colaborar, disfrutar de juegos con varios participantes, transferir archivos o comunicarse de alguna otra forma entre sí, utilizando sus PCs o dispositivos inteligentes de manera inalámbrica.

Aunque las redes LAN inalámbricas no son nada nuevo, su uso se ha visto reducido a los entornos de oficina debido tanto a limitaciones de velocidad como al hecho de que la mayoría de las personas no necesitaban hasta ahora un acceso móvil a la red. Por otro lado, las redes inalámbricas han visto su espacio natural de expansión en entornos de oficinas múltiples o universitarios, donde la alta movilidad de los usuarios justifica las presencia de redes inalámbricas. La cada vez mayor movilidad en el ámbito de los negocios va a provocar un aumento de la demanda en esta tecnología, cosa que ya se ha puesto de manifiesto en los últimos doce meses.

La comunicación inalámbrica, lo mismo que Internet, está diseñada como una tecnología de banda ancha compartida. Los usuarios se conectan a través de una Tarjeta de Interface de Red o NIC (Network Interface Card) a una Estación Base, que

ofrece la cobertura necesaria a través de una antena a los usuarios incluidos en su ámbito. Hasta el año 2000, estos sistemas compartidos ofrecían aproximadamente 1.5 Mbps de ancho de banda. En realidad, debido a interferencias y a la distancia, muchos usuarios sólo obtendrían una tercera parte de este ancho de banda disponible y tendrían entonces que compartirlo con otros.

En otras palabras, la comunicación inalámbrica no ofrecía ni con mucho el rendimiento de una red de cable. Además, las soluciones inalámbricas no disponían de la tecnología para segmentar el ancho de banda y aumentar el rendimiento en la forma en que podían hacerlo los conmutadores y los routers de cable.

Durante el pasado año, el rendimiento de las redes inalámbricas se ha incrementado hasta los a 11 Mbps. Este aumento hizo que muchas compañías hayan tenido en consideración las soluciones inalámbricas. Ahora era posible conectar a un usuario de PC típico a una red inalámbrica y permitirle acceder a todas las aplicaciones y servicios que necesitaba. La comunicación inalámbrica había alcanzado por decirlo de alguna manera la mayoría de edad.

En Estados Unidos, los ámbitos en donde se está haciendo un mayor uso de estas soluciones son los centros educativos y sanitarios; ambos con las mismas características de unos empleados móviles, un entorno en tránsito y la posibiliodad de trasladar servicios informáticos con rapidez.

La informática inalámbrica se convirtió en el sueño hecho realidad para los empleados "móviles", con conexiones de alto rendimiento movilidad y flexibilidad totales. Además, no se requería la ayuda técnica cuando se realizaban adiciones, traslados y cambios.

2.1 Topología y componentes de una LAN híbrida

Redes híbridas

Lo anterior dio lugar a la aparición de algunas redes híbridas cable/inalámbricas muy grandes. La parte de red de cableado continúa siendo necesaria, al tener que interconectar las estaciones inalámbricas de base, y eso se lleva a cabo utilizando cableado Ethernet estándar. Una red inalámbrica aprovecha la planta de cableado actual, y permite la distribución de estaciones de base inalámbricas (puntos de acceso) en los extremos de cables 10 Mbps Ethernet. Las estaciones de base tienen el tamaño aproximado de un detector de humos y pueden instalarse en paredes o techos. Una de las ventajas clave que aportan algunos vendedores es la posibilidad de alimentar la estación de base desde el cable Ethernet, eliminando la necesidad de sistemas de alimentación adicionales o externos o tomas de corriente. Por lo tanto, dondequiera que esté disponible un cable Ethernet se dispondrá de un punto de acceso inalámbrico capaz de dar servicio a muchos usuarios.

Esta capacidad es extraordinariamente valiosa en el despliegue de redes LAN inalámbricas, ya que no existen muchas tomas de corriente en los techos o a 2 metros

de altura en las paredes en que instalar un punto de acceso para maximizar la cobertura. Por lo tanto, eliminar la necesidad de un sistema de alimentación externo es una enorme ventaja y convierte a la comunicación inalámbrica en una solución verdaderamente flexible.

"La ausencia de un requerimiento conexión de potencia reduce las posibilidades de una colisión entre dos redes en una red LAN híbrida, teniendo en cuenta especialmente que la red inalámbrica continúa dependiendo de la infraestructura de cable para las intercomunicaciones("Aguirre José E. (2000).Redes Inalámbricas. URL; http://wwww.lafacu.com/apuntes/informatica/redes_inalamb/default.htm").

11 Mbps es sólo el comienzo para las comunicaciones inalámbricas, ya que el año 2001 trajo el nuevo estándar de 54 Mbps y permitió acumular más puntos de acceso para soportar a más usuarios. La comunicación inalámbrica va a adoptar muchas de las características de los conmutadores y routers de cable, con priorización avanzada de tráfico y capacidades de control. En otras palabras, una red inalámbrica tendrá tantas capacidades como una alternativa alámbrica.

Las cuestiones que se plantean hoy son: ¿Serán las redes alámbricas ya instaladas totalmente redundantes debido a las soluciones inalámbricas? ¿Eliminarán las redes inalámbricas la necesidad de una inversión adicional en cableado en el futuro? La respuesta al posible dominio inalámbrico sería que sí, pero no por mucho tiempo.

¿Sustituirán las redes inalámbricas a las redes de cable?

Las redes de cable tardarán aún algún tiempo en ser redundantes, aunque incluso hoy algunos entornos resultan realmente adecuados para la comunicación inalámbrica. Los edificios cuyo cableado resulta costoso y difícil son candidatos excelentes para soluciones inalámbricas, sin embargo, para las demandas de ancho de banda más elevadas - como el video garantizado, por ejemplo - la solución alámbrica continúa siendo la ganadora, con su velocidad de 100 Mbps frente a los 54 Mbps como máximo actuales de la solución inalámbrica.

Las compañías han invertido además mucho dinero en sus plantas de cableado actuales y en los equipos de comunicaciones que las conectan. Y como se sienten confortables en un entorno de cable, la necesidad (o el deseo) de cambiar no es tan fuerte como en las compañías que no tienen una necesidad obvia y determinante de hacerlo.

Investigaciones recientes muestran que aproximadamente un 15% de las compañías poseen algunas capacidades inalámbricas, y que más de un 50% de los administradores de sistemas tienen la intención de implementar una solución inalámbrica a corto o medio plazo. Por lo tanto, el deseo existe, y el mundo inalámbrico va a ser explotado en muchas áreas de negocio.

Sin embargo, este aumento en las comunicaciones inalámbricas no plantea una amenaza al cableado ni a las compañías de cableado, sino que ofrece una oportunidad. Las redes inalámbricas, y la necesidad de implementar soluciones híbridas, significan que las soluciones inalámbricas se convierten en una fuente potencial de ingresos para las compañías de cableado y permitirán incluso a las

compañías de cableado competir con los grandes proveedores de servicios en las redes de campus e incluso en las redes remotas.

2.2 Retos de configuración

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Optica logran velocidades aún mayores, y pensando a futuro se espera que las redes inalámbricas alcancen velocidades de sólo 10 Mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

1. *De Larga Distancia*.- “Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Area Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps” . [Black Uyless, 1997]

2. *De Corta Distancia*.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).

Las velocidades de transmisión son bajas.

Estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas, planos, etc.. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas: Red Pública De Conmutación De Paquetes Por Radio. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringidas por la propia organización de sus sistemas de cómputo.

Redes Públicas de radio

Las redes públicas tienen dos protagonistas principales: "ARDIS" (una asociación de Motorola e IBM) y "Ram Mobile Data" (desarrollado por Ericcson AB, denominado MOBITEX). Este ultimo es el más utilizado en Europa. Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia. La compañía proporciona la infraestructura de la red, se incluye controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas, estos sistemas soportan el estándar de conmutación de paquetes X.25, así como su propia estructura de paquetes. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

Los fabricantes de equipos de computo venden periféricos para estas redes (IBM desarrollo su "PCRadio" para utilizarla con ARDIS y otras redes, públicas y privadas). La PCRadio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta). Las redes públicas de radio como ARDIS y MOBITEX jugarán un papel significativo en el mercado de redes de área local (LAN´s) especialmente para corporaciones de gran tamaño.

Redes de área local (LAN).

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

Redes Infrarrojas

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un sólo cuarto o piso, algunas

compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios. Las transmisiones de radio frecuencia tienen una desventaja: que los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar, al momento de realizar este trabajo ya se han reunido varios países para tratar de organizarse en cuanto a que frecuencias pueden utilizar cada uno.

La transmisión Infrarroja no tiene este inconveniente por lo tanto es actualmente una alternativa para las Redes Inalámbricas. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de Redes, se utiliza un "transreceptor" que envía un haz de Luz Infrarroja, hacia otro que la recibe. “La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente”. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Las primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor. En la actualidad Photonics a desarrollado una versión AppleTalk/LocalTalk del transreceptor que opera a 230 Kbps. El sistema tiene un rango de 200 mts. Además la tecnología se ha mejorado utilizando un transreceptor que difunde el haz en todo el cuarto y es recogido mediante otros transreceptores. “El grupo de trabajo de Red Inalámbrica IEEE 802.11 está trabajando en una capa estándar MAC para Redes Infrarrojas”.

Redes de radiofrecuencia

Por el otro lado para las Redes Inalámbricas de RadioFrecuencia , “la FCC permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia : 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales” (“Martinez Mendez Francisco J. (2003) Telemática y teledocumentación: modelos de referencia. URL; http://um.es/~gtiweb/fjmm/ttsiteplan2/modelos.htm#inicio”). Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera. Para minimizar la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada spread-spectrum modulation, la cual tiene potencia de transmisión máxima de 1 Watt. deberá ser utilizada en la banda ISM. Esta técnica ha sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida

con un mínimo de interferencia. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente :
.

A) La secuencia directa: en este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

B) El salto de frecuencia: "este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada". Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 Mhz que son utilizadas por hornos de Microondas("Martinez Mendez Francisco J. (2003) Telemática y teledocumentación: modelos de referencia. URL; http://um.es/~gtiweb/fjmm/ttsiteplan2/modelos.htm#inicio")..

Las ventajas de las Redes de Area Local Inalámbricas (LAN´s) sobre las cableadas son: flexibilidad en la localización de la estación, fácil instalación y menores tiempos en la reconfiguración.

Las tecnologías para las LAN´s inalámbricas son dos: Infrarrojas y Radio Frecuencia. El grupo IEEE 802.11 está desarrollando normas para LAN´s inalámbricas. Ellos planean introducir una nueva subcapa de Control De Acceso al Medio (MAC) que tenga capacidad de accesar varios medios de transmisión y que tenga un rango aceptable para los requerimientos del usuario. No es fácil para el grupo tratar de rehusar alguna de las subcapas MAC existentes. Por dos razones principales:

1.- El rango de requerimientos de usuario impiden el soporte simultáneo de estaciones fijas, moviles y estaciones vehiculares.

2.- El permitir múltiples medios de transmisión, especialmente en la tecnología de radio frecuencia, el cual requiere de complicadas estrategias para cubrir la variación del tiempo en el canal de transmisión.

Así las LAN´s inalámbricas, únicamente son compatibles con las LAN´s cableadas existentes (incluyendo Ethernet) en la Subcapa de Control de Enlaces Lógicos (LLC). Sin embargo por restricciones, el rango de aplicaciones de éstas requieren estaciones fijas y por reordenamiento, para la tecnología infrarroja, es posible rehusar cualquiera de las Subcapas MAC.

Se propondrán algunas soluciones para la introducción de células infrarrojas dentro de redes Ethernet existentes (10Base5 ó 10base2). Se incluirá la presentación de la topología de LAN híbrida y los nuevos componentes requeridos para soportarla. Las LANs híbridas permitirán una evolución de las redes LANs IEEE 802.11.

Descripción de Ethernet

Ethernet es una topología de red que basa su operación en el protocolo MAC CSMA/CD. En una implementación "Ethernet CSMA/CD", una estación con un paquete listo para enviar, retarda la transmisión hasta que "sense" o verifique que el medio por el cual se va a trasmitir, se encuentre libre o desocupado. Después de comenzar la transmisión existe un tiempo muy corto en el que una colisión puede ocurrir, este es el tiempo requerido por las estaciones de la red para "sensar" en el medio de transmisión el paquete enviado. En una colisión las estaciones dejan de transmitir, esperan un tiempo aleatorio y entonces vuelven a sensar el medio de transmisión para determinar si ya se encuentra desocupado.

Una correcta operación, requiere que las colisiones sean detectadas antes de que la transmisión sea detenida y también que la longitud de un paquete colisionado no exceda la longitud del paquete. Estos requerimientos de coordinación son el factor limitante del espacio de la red. “En un cableado Ethernet el medio coaxial es partido en segmentos, se permite un máximo de 5 segmentos entre 2 estaciones. De esos segmentos únicamente 3 pueden ser coaxiales, los otros 2 deben de tener un enlace punto-a-punto.

Los segmentos coaxiales son conectados por medio de repetidores, un máximo de 4 repetidores pueden ser instalados entre 2 estaciones”[Palazón, 2002]. La longitud máxima de cada segmento es:

1.- 500 mts para 10Base5
2.-185 mts para l0Base2.

La función del repetidor es regenerar y retransmitir las señales que viajen entre diferentes segmentos, y detectar colisiones.

Topología y componentes de una LAN híbrida

En el proceso de definición de una Red Inalámbrica Ethernet se debe olvidar la existencia del cable, debido a que los componentes y diseños son completamente nuevos. Respecto al CSMA/CD los procedimientos de la subcapa MAC usa valores ya definidos para garantizar la compatibilidad con la capa MAC. La máxima compatibilidad con las redes Ethernet cableadas es, que se mantiene la segmentación.

Además las células de infrarrojos requieren de conexiones cableadas para la comunicación entre sí. La radiación infrarroja no puede penetrar obstáculos opacos. Una LAN híbrida (Infrarrojos/Coaxial) no observa la estructura de segmentación de la Ethernet cableada pero toma ventaja de estos segmentos para interconectar diferentes células infrarrojas.

La convivencia de estaciones cableadas e inalámbricas en el mismo segmento es posible y células infrarrojas localizadas en diferentes segmentos pueden comunicarse por medio de un repetidor Ethernet tradicional.

En comparación con los componentes de una Ethernet cableada (Por ejemplo MAU´S, Repetidores), 2 nuevos componentes son requeridos para soportar la Red híbrida. Un componente para adaptar la estación al medio óptico, la Unidad Adaptadora al Medio Infrarrojo (IRMAU), descendiente del MAU coaxial, y otro componente para el puente del nivel físico, del coaxial al óptico, la Unidad Convertidora al Medio (MCU), descendiente del repetidor Ethernet. La operación de estos componentes es diferente para las células basadas en reflexión activa (satélite) y las de reflexión pasiva.

Rango dinámico en redes ópticas CSMA/CD

En las redes ópticas CSMA/CD el proceso de detección de colisión puede ser minimizado por el rango dinámico del medio óptico. El nivel del poder de recepción óptico en una estación puede variar con la posición de la estación; y existe la probabilidad de que una colisión sea considerada como una transmisión fuerte y consecuentemente no sea detectada como colisión. El confundir colisiones disminuye la efectividad de la red. Mientras el rango dinámico incremente y el porcentaje de detección de colisión tienda a cero, se tenderá al protocolo de CSMA.

"En las redes inalámbricas infrarrojas basadas en modos de radiación cuasi-difuso, el rango dinámico puede ser menor en las células basadas en satélites que en las basadas en reflexión pasiva. En las células basadas en satélites, el rango dinámico puede reducirse por la correcta orientación de receptores/emisores que forman la interface óptica del Satélite. En una célula basada en reflexión pasiva el rango dinámico es principalmente determinado por las propiedades de difusión de la superficie reflexiva". [Palazón, Francisco J., 2002]

Operación y caracterestícas del IRMAU

La operación de IRMAU es muy similar al MAU coaxial. Unicamente el PMA (Conexión al Medio Físico).y el MDI (Interfase Dependiente del Medio) son diferentes. El IRMAU debe de tener las siguientes funciones :

I. Recepción con Convertidor Óptico-a-Eléctrico.
II. Transmisión con Convertidor Eléctrico-a-Optico
III. Detección y resolución de colisiones.

El IRMAU es compatible con las estaciones Ethernet en la Unidad de Acoplamiento de la Interfase. (AUI). Esto permite utilizar tarjetas Ethernet ya existentes. Para las estaciones inalámbricas no es necesario permitir una longitud de cable de 50 mts., como en Ethernet. La longitud máxima del cable transreceptor debe estar a pocos metros (3 como máximo). Esto será suficiente para soportar las separaciones físicas entre estaciones e IRMAU con la ventaja de reducir considerablemente los niveles de distorsión y propagación que son generados por el cable transreceptor. Los IRMAUs basados en células de satélite ó reflexión pasiva difieren en el nivel de poder óptico de emisión y en la implementación del método de detección de colisiones.

Configuración de una red Ethernet híbrida

Los nuevos componentes imponen restricciones a la máxima extensión física de la red, como se mencionó un Ethernet coaxial puede tener un máximo de 5 segmentos (3

coaxiales) y 4 repetidores entre 2 estaciones. La Ethernet híbrida debe de respetar estas reglas.

Ahora un MCU será como un repetidor coaxial al momento de la definición de la red, con funciones similares. Algunas restricciones resultan de este factor, dado que la transformación de un paquete entre dos estaciones inalámbricas de diferentes células, se transportará a través de dos MCUs, por ejemplo, si se requiere que 3 segmentos deban de soportar células infrarrojas (segmentos híbridos), entonces el enlace punto-a-punto no puede ser utilizado entre estos segmentos.

La extensión máxima de una red híbrida se obtiene cuando un segmento es híbrido.

Capítulo 3 Medidas de seguridad en una red inalámbrica

Una de las preguntas más frecuentes en cuanto a redes inalámbricas, es "¿Qué hay con la seguridad?". Estos días, lo más inteligente que puede hacer cualquier administrador de redes, es preocuparse por la seguridad. Desafortunadamente, empleados descontentos, hackers, virus, espionaje industrial, y otras formas de ataque no son poco comunes en nuestras redes. Ahora bien, cuales son las amenazas a la seguridad que tiene cualquier red, y como se relacionan específicamente al aspecto de las redes inalámbricas, así como los puntos exclusivos para las redes inalámbricas, ya sea que estén integrados en la tecnología o como agregados, para poder combatir estas amenazas potenciales.

La mayoría de las personas sienten seguridad cuando están utilizando una red alámbrica, pero tan pronto como los datos comienzan a viajar a través del "aire", se preocupan. Después de todo, lo que se piensa es, la red alámbrica se encuentra dentro de sus instalaciones, y eso hace pensar que ya tiene algún elemento extra de seguridad.

La verdad, es que cualquier red, incluida una red alámbrica, esta sujeta a potenciales riesgos de seguridad:

- Ataques desde dentro del grupo de usuarios de la red
- Acceso no autorizado
- Fuga de información hacia fuera de la compañía

Las buenas noticias es que hay formas de combatir estas amenazas para redes tanto alámbricas como inalámbricas y, de hecho, los segmentos de redes inalámbricas incluyen algunas funciones de seguridad incluidas que tal vez no tengamos consideradas

La comodidad de prender nuestra laptop en algún lugar dentro de la escuela donde sabemos que hay un punto de acceso (AP) y conectarnos a la intranet de nuestro trabajo, enviar información, revisar correos o simplemente conectarnos a un mensajero X para saludar a alguien, es una de las grandes ventajas que nos brindan las redes inalámbricas.

3.1 Seguridad para redes inalámbricas

Por siempre, una de las mas grandes amenazas de las redes en cualquier lugar, viene desde dentro de la misma. Sin las medidas de seguridad adecuada, cualquier usuario registrado de la red puede acceder a datos a los que el/ella no debe tener ningún acceso.

El Personal involucrado inconforme, puede haber descubierto la forma de leer, distribuir e incluso, alterar archivos de datos de información crítica. Los administradores de red, independientemente de si tienen segmentos de redes alámbricas o inalámbricas, necesitan contar con las herramientas de seguridad para sus ambientes, los niveles de seguridad adecuados para cada usuario, y una forma eficiente de auditar constantemente la efectividad de la seguridad. Otra área de preocupación en cuanto a la seguridad si no es que la más grande en este momento - para cualquier administrador de red, es el crecimiento que está teniendo internet. Si los usuarios de la red interna pueden salir a internet, eso quiere decir, que los usuarios de afuera, pueden entrar a la red si no tomamos las precauciones necesarias. Y eso aplica no sólo a la internet, si no a cualquier medio con que contemos para permitir que cualquier usuario desde afuera pueda comunicarse hacia el interior de la red. Los productos para Acceso Remoto que permiten al personal de ventas o de marketing acceder a la red por medio de dial-up para revisar sus correos o sincronizar archivos, las oficinas remotas que se pueden conectar a través de MODEM, los Websites y las " Extranets " que conectan a nuestros clientes y/o proveedores a nuestra red, todos estos medios, pueden dejar nuestra red vulnerable para ataques de hackers, virus o cualquier otro intruso. Existen actualmente muchos productos y herramientas para permitir a los administradores de la red asegurar las redes en prevención de estas amenazas.

La autenticación de usuarios y sus políticas, son administradas principalmente por el sistema operativo, y puede mejorar si agregamos productos de terceros.

Los Firewall (pared de fuego), ofrecen una protección adicional. Quizás la mayor amenaza, o cuando menos la más difícil de proteger, es cuando alguien esta solamente husmeando entre los paquetes de datos.

Actualmente, las redes alámbricas se encuentran "algo" vulnerables a estas fugas de información. La mayoría de las tarjetas de red que hay en el mercado actualmente, pueden trabajar en " modo promiscuo ", esto quiere decir, que con el software adecuado, les permite capturar todos los paquetes de datos que circulen en la red. ¿Qué administrador de red actualmente no posee algún tipo de "sniffer" (husmeador) para detectar problemas en la red?. Afortunadamente un buen software de "sniffer" tiene aún un costo relativamente alto para que cualquier persona lo adquiera a menos que tenga una razón fuerte. Estos programas, lo que hacen es leer, capturar y organizar cualquier tipo de dato que haya cruzado por la red. El cable Ethernet 10Base-T funciona como cualquier antena (evidentemente, para que esto no suceda, existen especificaciones que se deben cumplir). En un caso así, cualquier con suficiente motivación y con una buena antena, así como con equipo especial, podría sentarse fuera del edificio y capturar algo de su tráfico de datos. En realidad, en este caso, para que una red sea 100% segura, se debe de contar con algún mecanismo de encriptación.

3.2 Métodos para identificación de red

Las consideraciones de seguridad impactan a toda la infraestructura de red. Si la seguridad es una preocupación, deberán considerar soluciones y herramientas para ambos segmentos, las redes inalámbricas y las alámbricas. De hecho, la tecnología inalámbrica por si misma, y en particular, la tecnología disponible hoy para implementaciones de Lan, ofrecen algunas características que agregan algo extra de seguridad a las redes inalámbricas. La tecnología de Espectro Disperso de Salto de Frecuencia (Frequency Hopping Spread Spectrum - FHSS) en si misma; el Identificador del Conjunto de Servicios Extendidos (Extended Service Set Identifier - ESS ID); una contraseña de usuario; la facilidad de agregar algún producto de encriptación de terceros. Esta tecnología de espectro disperso fue introducida hace aproximadamente 50 años por los militares como una forma segura de enviar y recibir comunicaciones. Desde el principio (y debido a su naturaleza) fue concebida para ser resistente al ruido, las interferencias, el bloqueo o la detección no autorizada. Los transmisores de espectro disperso, envían sus señales a través de un rango de frecuencias a bajo poder, en contraste con otras tecnologías (como microondas) que concentran todo su poder en una sola frecuencia.

Hay varias formas de implementar la transmisión por medio de espectro disperso, las dos mas comunes, son la secuencia directa y el salto de frecuencia. Nos enfocaremos en el salto de frecuencia, pues al parecer es mas seguro. Muchos productos utilizan el salto de frecuencia (Frecuency Hopping) como el método de transmisión de sus señales, existen diferentes frecuencias que pueden utilizar, en este caso, y centrandonos un poco más en los servicios que se están ofreciendo ahora de Banda Ancha, se tomará el caso específico de México (aunque creo que en la mayoría de los países utilizan el mismo rango de frecuencias). El rango de frecuencias que se usan actualmente se encuentra en el rango de las frecuencias disponibles para la banda ICM “(Industrial Científica y Medica - ISM en inglés) que va de los 2.400 - 2.483 GHz, la cual dividen en series de hasta 79 canales distintos y separados. Las transmisiones son enviadas por cada canal en secuencia aleatoria (llamada "secuencia pseudo-aleatoria") como primero el canal 1, luego el canal 32, canal 3, canal 56, etc. Los radios cambian de frecuencia varias veces en un segundo, transmitiendo en cada canal por un periodo específico , y luego se cambian al siguiente canal en la secuencia y así, hasta cubrir todos los canales y después volver a repetir la secuencia. Sin conocer cuanto tiempo la señal permanecerá en un canal (llamado " dwell time ") y cual es el patrón de saltos, es prácticamente imposible para una estación "no asociada" el recibir y descifrar los datos.” (“Merike Kaeo , Diseño de seguridad en redes, 2003, pág. 146”).

El uso de diferentes patrones de salto, dwell times , y/o el número de canales, es lo que permite a más de dos redes inalámbricas independientes convivir una junto a la otra sin causarse interferencia y sin temor a que los datos de una red puedan ser enviados a la otra. Para que cualquier estación pueda tener acceso a algún AP, primero se debe determinar si la estación pertenece a su red o a su Conjunto Extendido de Servicios (Extended Service Set - ESS).

El AP primero revisa si el identificador de ESS de la estación (comúnmente de 32 caracteres) concuerda con el suyo. Los que no son miembros, aún siendo el mismo fabricante y mismo modelo del AP, no podrán participar en la red y por lo tanto no podrán contar con el patrón de saltos y el dwell time , por lo que no podrán recibir ni enviar ningún paquete de datos.

Como medida adicional, este identificador, sólo podrá ser cambiado al administrar el equipo en cuestión con privilegios de administrador y algunos fabricantes, solo permiten este cambio al estar conectados físicamente al equipo, nunca de manera remota. Si hay la necesidad de tener dos segmentos de red separados en una sola red, como por ejemplo, un segmento para contabilidad y el resto para los demás, entonces basta con programar los ESS ID diferentes.

Con un ESS ID de 32 caracteres y una secuencia de salto de 3 dígitos, es posible darnos cuenta la difícil que sería para cualquiera adivinar el ESS ID exacto (siempre y cuando no utilicen algo como "bond" o "007" o el nombre de su compañía) y la secuencia de salto para poder obtener acceso a la LAN por medio de cualquiera de sus segmentos inalámbricos ya sea por autenticación de Usuarios o control de contraseñas, aunque no es específico de las LAN inalámbricas, si se recomienda el uso de contraseñas de red en todas las estaciones inalámbricas. Cualquier sistema operativo cuenta con niveles de seguridad y administración de usuarios.

Aquí es un poco mas necesario, ya que en una red inalámbrica, es de suponerse que los usuarios se encuentran en movimiento y por lo tanto, moviendo sus equipos de una ubicación a otra, por lo que una política de contraseñas exigente agrega un nivel más de seguridad al garantizar que la estación esta siendo usada por la persona que se supone debe hacerlo.

El siguiente nivel es la encriptación de datos, si sus necesidades, son de mantener sus datos totalmente secretos o confidenciales, como en el caso de las agencias militares y algunas financieras, entonces seguramente necesitaran tomar medidas extras. El último y mas alto nivel de seguridad es agregando algún producto de encriptación de datos en toda la red como un todo. Ya sea por software o por hardware, el paquete de datos, será codificado antes de ser enviado hacia la Lan. Solo las estaciones que tengan la llave de desencriptación correcta, podrá decodificar el mensaje y leer los datos. Si la seguridad total es necesaria, entonces la encriptación de datos es la mejor solución. Algunas de estas capacidades se encuentran ya en algunos sistemas operativos. Otras consideraciones de las redes inalámbricas es que cuentan con otras características que las hace un poco menos preocupantes en cuanto a seguridad. Por ejemplo, algunos AP, filtran el tráfico de red que no va dirigido a las estaciones inalámbricas asociadas. Esto quiere decir que la mayoría del tráfico de red nunca saldrá al "aire". Por otro lado, los equipos inalámbricos tienen un rango de transmisión limitado, dependiendo del entorno, por lo que si alguien deseara "escuchar" algo de la señal, debiera estar relativamente cerca. Y por último, los usuarios de servicios inalámbricos pueden estarse moviendo de un AP a otro durante una misma sesión, y en este caso, el tráfico de red nunca será transmitido al utilizar el mismo patrón de saltos que antes, haciendo que el "escuchar" (eavesdropping) sea prácticamente imposible. WEP - Wired Equivalency Privacy El comité de IEEE 802.11 es responsable por fijar los estándares para las redes inalámbricas y la mayoría de los

productos que se encuentran en el mercado actualmente fueron diseñados y fabricados para cumplir con el estándar. Esta organización ha tocado los puntos respecto a la seguridad creando la "Equivalencia Alámbrica Privada" (Wired Equivalency Privacy - WEP). Usuarios preocupados por el acceso no autorizado se preocupan porque algún intruso no sea capaz de acceder a la red utilizando un equipo similar (o igual) al que utilizamos en nuestra LAN, o bien capturar el tráfico de red que viaja via inalámbrica en la misma (eavesdropping).

En las redes 802.11, el acceso a los recursos de la red, está prohibido para cualquier usuario que no conozca o no pruebe conocer las "llaves" actuales. La mayoría de las marcas ofrecen este nivel extra de seguridad agregando una contraseña de autenticación proporcionando las "llaves" correctas de acceso al AP y a toda la red. El eavesdropping es prevenido por el algoritmo de WEP en donde un generador de números aleatorios es inicializado por medio de una llave secreta. Este simple algoritmo tiene las siguientes propiedades: · Razonablemente Fuerte . Un ataque de fuerza bruta a este algoritmo es difícil debido a que cada frame es mandado con un vector de inicialización el cual reinicia el PRNG para cada frame.

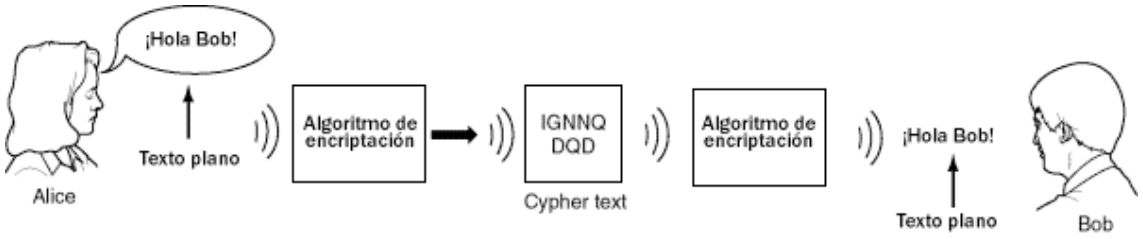
Auto Sincronización . Debido a que al igual que en cualquier LAN las estaciones inalámbricas trabajan en un medio que puede perder la conexión por cualquier causa y los paquetes se pierden, el algoritmo de WEP re-sincroniza en cada mensaje que manda. Por lo cual se concluye un cierto nivel de seguridad es necesario en la mayoría de las redes Lan, sin importar si son alámbricas o inalámbricas. Aún las redes alámbricas son vulnerables a la curiosidad de alguien interno, algún ataque externo e incluso el pegarse a la red alámbricamente (wire-tapping). Nadie quiere arriesgarse a tener una Lan expuesta a algún observador casual o abierta a alguna persona no deseada. Pero si la información es demasiado confidencial, entonces cualquier medida extra debe ser tomada para asegurar la privacidad.

3.3 Encriptación de información y sus problemas

La encriptación incluye codificar datos usando una clave de tal manera que un escuchador furtivo no pueda fácilmente leer los datos. A estos datos encriptados se les refiere como texto de código o ciphertext mientras que a los datos originales se les refiere como texto plano o *plaintext*. Al proceso de ir de *ciphertext* a plaintext se le refiere como desencriptación. La Figura 3.1 representa a la pareja de criptografía clásica, Alice y Bob, que se comunican por medio del Caesar Cipher. El Caesar Cipher es un simple criptosistema que alterna los datos; en este caso, dos letras hacia adelante. Obviamente, este no es un algoritmo de encriptación seguro. El medio más popular para medir la seguridad de un algoritmo de encriptación es que es computacionalmente seguro. Un algoritmo de encriptación es computacionalmente seguro si el sistema no puede ser interrumpido por análisis sistemático con los recursos disponibles. Hay dos categorías generales de encriptación:

- Encriptación de clave privada y clave pública. Además de encriptar un mensaje completo, ambos tipos de encriptación pueden ser empleados para firmar un documento digitalmente.

- La siguiente sección examina la encriptación asimétrica y usa RSA como un ejemplo. Ambos ejemplos presentados son computacionalmente seguros cuando se está usando una clave significativamente larga.



Elaborado por: **(“**Morguet Carlos V. (2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php”)

Fig..3.1

Encriptación simétrica

La encriptación simétrica se refiere a algoritmos de encriptación donde el algoritmo de encriptación y desencriptación utilizan la misma clave. Específicamente:

E(p,k)=C & D(C,k)=p
Donde
E = algoritmo de encriptación,
D = algoritmo de decriptación,
P = texto plano o plaintext (datos originales),
K = clave de encriptación y
C = código de texto o ciphertext

Ya que se utiliza la misma clave para encriptar y desencriptar los datos, esta clave se debe mantener en privado. A este tipo de encriptación se le refiere también como encriptación de clave secreta así como encriptación convencional. Una de las dificultades de usar un sistema tal es, ¡comunicar la clave! Una forma simple de superar el problema de intercambio de clave es primero usar la encriptación de clave pública para intercambiar claves y luego emplear la encriptación de clave privada. Esto también es muy práctico ya que la DESencriptación opera típicamente a aproximadamente 45,000 kbps y la criptografía de clave pública opera típicamente a 20 kbps. Ahora examinamos el algoritmo de encriptación de clave privada mas popular,

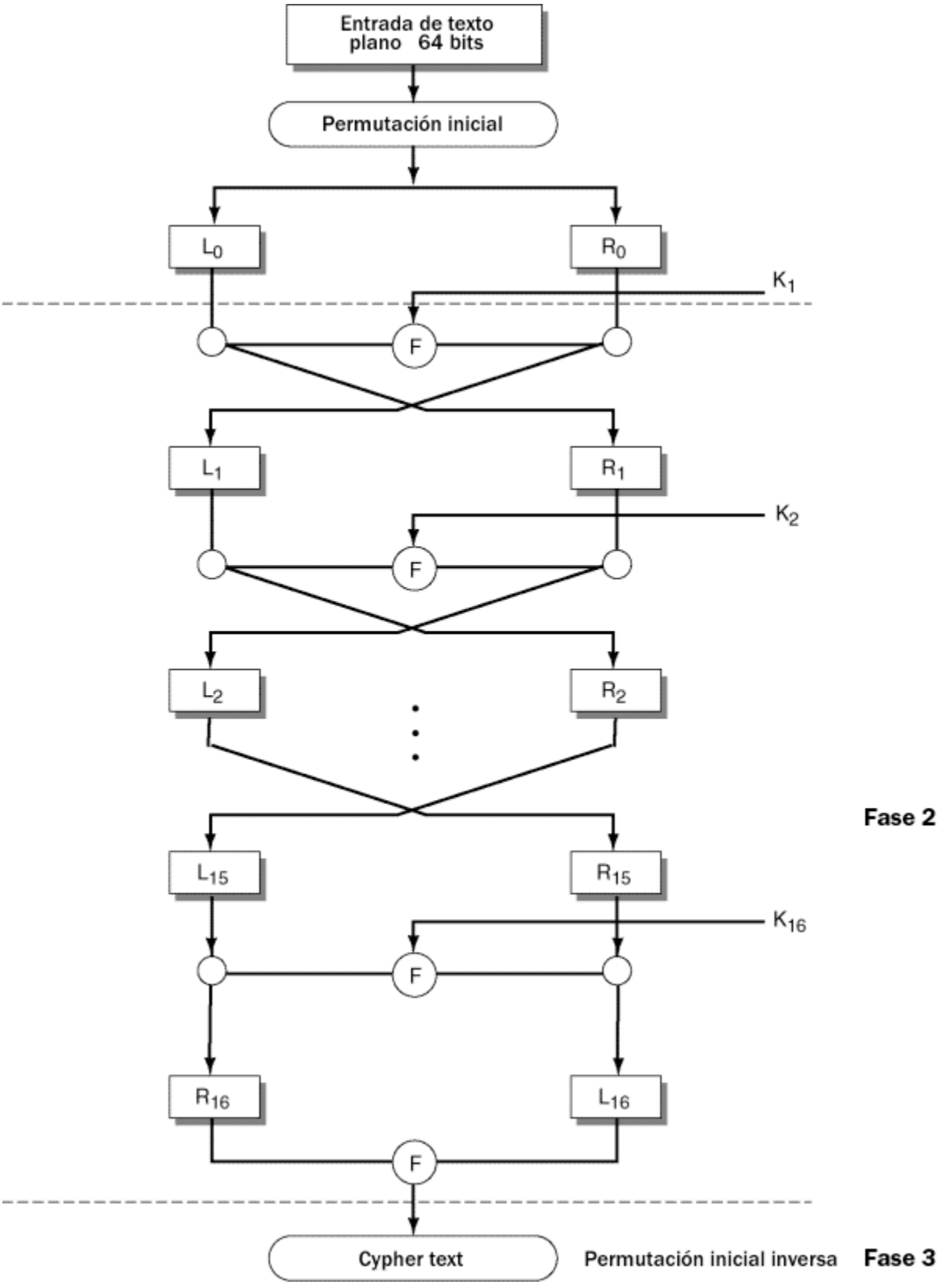
DES (pronunciado DEZ), el cual fue declarado el estándar de Estados Unidos por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology) (NIST) en 1977 [NIST77]. Otros algoritmos de encriptación de clave privada incluyen IDEA [Lai92] y Skipjack (usado en los chips clipper) [NIST94a].

Estándar de encriptación de datos

El DES fue implementado como un estándar en 1977 y es reafirmado cada cinco años, típicamente en Diciembre. Todas las agencias federales de Estados Unidos y otras organizaciones que procesan información a favor de ellas deben utilizar DES (para documentos no clasificados). Su uso es también común entre corporaciones no gubernamentales. Fue basado en el sistema Lucifer de IBM, el cual emplea una clave de 128 bits. Generalmente, entre más grande sea la clave, es más seguro el sistema. DES utiliza una clave de 64 bits; sin embargo, 8 bits son para detección de errores por eso efectivamente hace a DES un sistema de 56 bits para propósitos de seguridad.

Se le refiere como un código de bloque ya que encripta datos en bloques de 64 bits de datos binarios. La seguridad de DES está basada en el secreto de la clave, no en el secreto del algoritmo. La seguridad se aumenta más por el tamaño de la clave ya que hay setenta mil billones (70,000,000,000,000,000) de claves posibles; de ese modo, las oportunidades de obtener la clave son lo suficientemente bajas como para que sean seguras para la mayoría de los ambientes distribuidos. Por supuesto que con el poder de la PC promedio que se incrementa continuamente, la habilidad para buscar consecutivamente una clave y romper un código proporcionalmente está incrementándose también.

Hay tres fases para el algoritmo de encriptación, las cuales están descritas en la Figura 3.3.2. La desencriptación se logra realizando estas tres fases en orden regresivo incluyendo el uso de bloques de clave descritos en la fase 2 en orden regresivo (K16 a K1).


Entrada de texto plano 64 bits
Permutación inicial
L_0
R_0
K_1
F
L_1
R_1
K_2
F
L_2
R_2
L_{15}
R_{15}
K_{16}
F
R_{16}
L_{16}
F
Cypher text
Permutación inicial inversa
Fase 2
Fase 3

elaborado por:(“Morguet Carlos V. (2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php”)

Fig 3.2 Las tres fases de DES

La primera fase de DES comprende una permutación del bloque de 64 bits que cambia el orden de los bits dentro de cada bloque. El término permutación se usa en el estricto sentido matemático; solo cambia el orden. La permutación exacta está especificada por una tabla. Los 64 bits de datos se dividen en dos mitades: LO (mitad izquierda) y RO (mitad derecha). Los subíndices cero indican las mitades originales. Estos subíndices son incrementados después de cada repetición en la fase 2 del algoritmo DES.

La permutación DES

La tabla exacta usada por el estándar DES para la permutación inicial es representada en la Tabla 3.3 . De este modo, el primer bit después de las permutaciones fue el bit 58 antes de la permutación. El segundo bit después de la permutación fue el bit 50 antes de la permutación. El último bit de los datos permutados fue originalmente el bit de datos 7 del texto plano.

Tabla 3.3 Permutación inicial DES

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	14
62	54	46	38	30	22	14	16
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

DES Fase 2: Alternamiento o *shifting* (repetido 16 veces)

La segunda fase comprende un algoritmo dependiente de tablas que utiliza la clave. A esta acción generalmente se le refiere como cambiando los datos. El algoritmo se repite 16 veces, el cambio se comporta en forma diferente cada vez ya que utiliza un diferente sub-bloque de la clave. El sub-bloque de la clave se determina por otro

conjunto de tablas y por su propio algoritmo de cambio. Después de cada repetición, los subíndices de L (mitad izquierda) y R (mitad derecha) se incrementan para representar cada etapa. Al resultado después de la repetición 16 se le refiere como la preinformación de salida y se pasa a la fase 3.

DES Fase 3: Permutación invertida

La fase final de DES comprende una permutación del bloque de 64 bits que cambia el orden de los bits dentro de cada bloque igual como en la fase 1 pero utiliza una tabla diferente. La permutación exacta se especifica por una tabla (ver Tabla 2). La información de salida de esta permutación es el texto de código.

La permutación invertida de DES

La tabla exacta usada por el estándar DES para la permutación invertida final se representa en la Tabla 2 . De esta manera, el primer bit después de las permutaciones fue el bit 40 de la pre-información de salida. El segundo bit después de la permutación fue el bit 8 antes de la preinformación de salida. Finalmente, el último bit del texto de código fue el bit de datos 25 de la pre-información de salida.

Tabla 2 Permutación invertida de DES

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Firmas digitales con encriptación de clave simétrica

Cuando se envían datos a través de una red, hay dos métodos básicos para firmar un documento digitalmente. A una firma digital también se le refiere como un compendio de mensajes y emplea una función *hash* segura. A esta función *hash* se le refiere como una función de compendio y es típicamente de 128 bits de largo. La determinista función de compendio se aplica al documento completo y produce un valor que es dependiente de cada bit de información en el mensaje. Hay dos métodos para calcular el compendio utilizando una clave privada compartida. El método más fácil y

más rápido calcula un valor *hash* para el mensaje que es entonces encriptado por la clave privada. El mensaje es luego enviado con el compendio encriptado. El receptor puede entonces calcular el compendio del mensaje, encriptarlo y comparar valores. Si se igualan, el contenido del documento no ha sido alterado. El segundo método integra la clave privada al mensaje y luego calcula el valor *hash*. El resultado de este método es como sigue.

Calcule D(M,K) donde
D es la función de compendio
M es el mensaje y
K es la clave privada compartida

El documento puede entonces ser publicado y distribuido. Este compendio de mensaje tiene el beneficio adicional de prevenir la falsificación del valor de compendio mismo ya que las terceras personas no tienen conocimiento de la clave privada que se necesita para computar el valor de compendio correcto. En ambos casos, solo aquellos con conocimiento de la clave secreta pueden verificar su integridad, y todos los documentos fraudulentos son fácilmente detectados.

Encriptación asimétrica

La encriptación asimétrica incluye dos claves (una clave pública y una clave privada) y es también conocida como encriptación de clave pública. Si algo de información está encriptada con una clave pública, la correspondiente clave privada puede desencriptar la información como sigue.

E(p,ku)=C & D(C,kr)=p
Donde E = algoritmo de encriptación,
D = algoritmo de decriptación,
P = plaintext (datos originales),
Ku = clave públicas
Kr = clave privada y
C = ciphertext.

Si algo de información es encriptada con una clave privada, la correspondiente clave pública puede desencriptar la información como sigue.

E(p,kr)=C & D(C,ku)=p
Donde E = algoritmo de encriptación,
D = algoritmo de decriptación,
P = plaintext (datos originales),
Ku = clave públicas
Kr = clave privada y
C = ciphertext.

No se podra desencriptar un mensaje con la misma clave que se encriptó, como se representa en la Figura 3.4. Además, es matemáticamente difícil obtener una clave del

otro. La clave privada debe mantenerse en secreto por el usuario y de ese modo su nombre. Por supuesto, si todos supieran la clave privada, ¡no sería tan privada! La clave pública no se mantiene en secreto y puede hacerse disponible públicamente a través de un servicio de enlistado público, usualmente implementado usando X.509. La idea de encriptación de clave pública fue propuesta primero por Diffie Hellman en 1976 [DH76] en el contexto de un método para intercambio de claves. La forma más popular de criptografía de clave pública es RSA, la cual examinamos ahora en detalle.

RSA

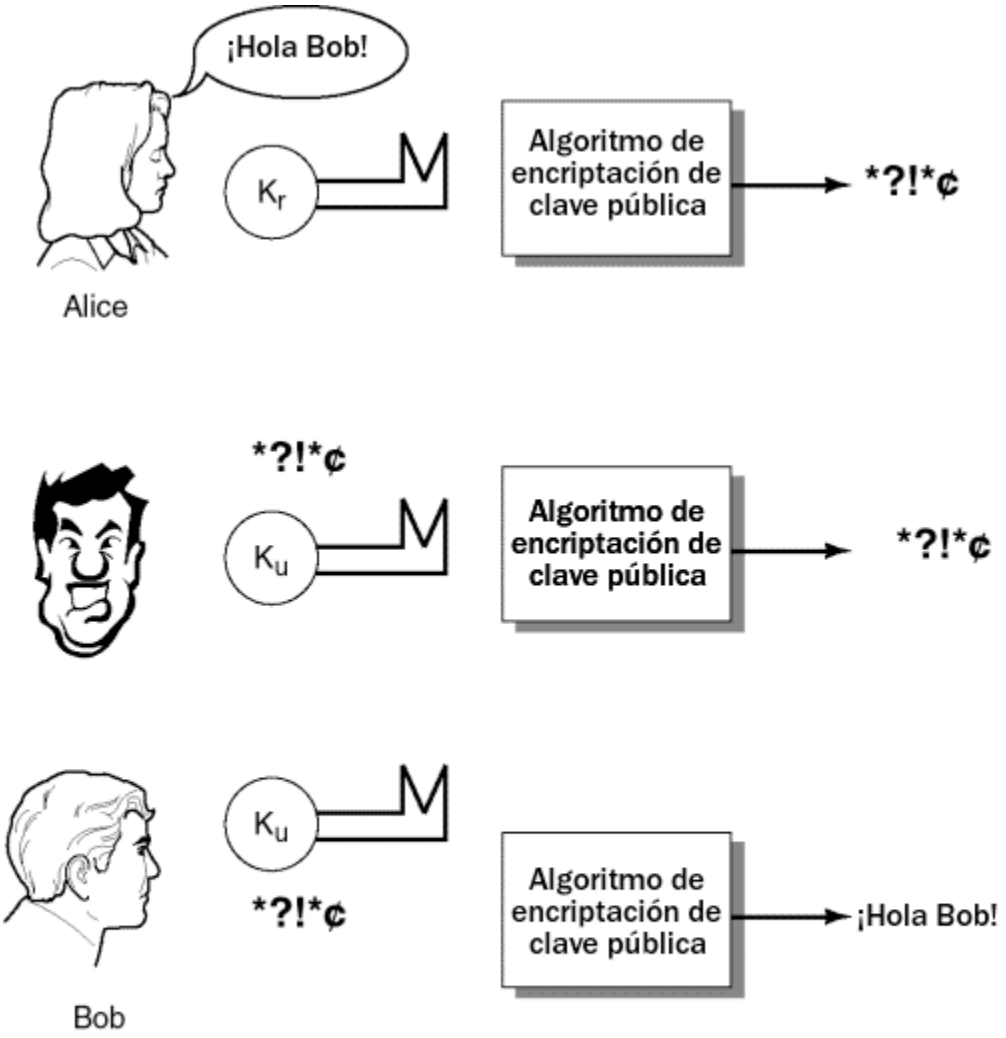
RSA es un algoritmo de encriptación de clave pública protegido por patente y desarrollado por Rivest, Shamir y Adleman en 1978. Hay tres fases para utilizar RSA. La fase 1 incluye la determinación de sus claves públicas y privadas. La fase 2 incluye encriptar un mensaje. Finalmente, la fase 3 incluye desencriptar un mensaje.

RSA Fase 1: Determinando sus claves públicas y privadas

Para derminar las claves públicas o privadas, casa usuario debe seguir estos pasos:

1. Seleccione dos números primos grandes, P y Q.
2. Calcule N = P*Q.
3. Calcule F(n) = (P - 1)(Q - 1).

La figura 3.5 muestra a continuación la criptografía de clave pública..



elaborado por:(**"**Morguet Carlos V. (2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php")

Figura 3.5 Criptografía de clave pública

4. Seleccione e, donde 1 <=e <=n-1 y GDC (e, F(n))=1.
5. Calcule d, donde ed= 1(mod f(n)) (usando el algoritmo euclidiano extendido).
6. Haga públicos d y n; estos valores constituyen la clave pública.

RSA Fase 2: Encriptando un mensaje.

Para encriptar el mensaje M usando RSA, donde 1 <=M <=N - 1 donde debe calcular lo siguiente.

C=Me (Mod N) donde C es su ciphertext. Send C.

RSA Fase 3: Decriptando el ciphertexto.

Para decriptar el ciphertexto C usando RSA, debe calcular lo siguiente.
Cd (Mod N) =M donde M es su plaintext original.

Firmas digitales con encriptación de clave pública

El método de encriptación de clave pública para firmas digitales emplea RSA. En este método el iniciador utiliza su clave privada para encriptar ya sea el archivo de datos completo (costoso) o su firma al archivo usando una función de compendio. El principal beneficio sobre la contraparte de clave privada es de que no hay problemas de distribución de claves. Un recipiente puede entonces utilizar la clave pública para desencriptar la firma o archivo y verificar su origen y/o contenido. Recordando que debido al intrincamiento de la criptografía de clave pública (solo la clave pública apropiada desencriptará el mensaje o el compendio). Finalmente, si está enviando un mensaje a alguien que tenga una clave pública conocida, se podrá encriptar el mensaje o el compendio con la clave pública del recipiente de modo que solo el recipiente pueda verificar el contenido utilizando su propia clave privada.

Una corporación puede seguir una política de seguridad estableciendo que "cualquier cosa que no sea explícitamente permitida no es permitida" y una universidad o sitio privado podría seguir al otro extremo. Específicamente, "cualquier cosa que no sea explícitamente desaprobado está bien". Frecuentemente, mientras que el control de acceso sea un concepto de sistema operativo, los sistemas operativos distribuidos de hoy deben depender en asistencia de *hardware*. En cualquier caso, el control de acceso en actuales sistemas distribuidos generalmente se logra por lo que es conocido como un *cortafuegos o firewall*.

Un *firewall* debe ser inmune a amenazas de seguridad y prevenir que pasen todas las amenazas de seguridad a través de la pared y sistema(s) que protege. Los *firewalls* no deben prevenir las actividades que conforman la política de seguridad de la organización.

Los *firewalls* generalmente encajan en una de las siguientes dos categorías.

1. *Gateways* de filtración de paquetes
2. Servicios proxy

Frecuentemente, una ubicación puede emplear ambos tipos de *firewalls* para realizar el control de acceso deseado. Examinamos cada una de las dos categorías básicas de *firewalls*.

Gateways de filtración de paquetes

Un *firewall* de gateway de filtración de paquetes incluye a un ingeniero de seguridad quien debe explícitamente establecer lo que puede pasar por la pared. Esto incluye que información interna puede salir del *firewalls* así como que ubicaciones externas se permiten a través del *firewalls*. Además, el ingeniero de seguridad puede configurar el *firewalls* para especificar que servicios computacionales internos pueden ser compartidos con el mundo exterior.

Los f*irewalls* de gateway de filtración de paquetes son generalmente implementados en el enrutador que conecta al sistema interno con el mundo exterior. Mientras que los enrutadores en general pueden desempeñar funciones de filtración de paquetes, los enrutadores *firewalls* tienden a proveer una mejor interfaz de usuario y son generalmente más fáciles de configurar para filtración basada en la seguridad. Al igual que los servicios postales alrededor del mundo requieren de direcciones en sobres, las redes requieren que los mensajes tengan direcciones. Son estas direcciones que este tipo de *firewalls* revisa contra su lista antes de permitir que un mensaje pase en cualquier dirección. Ya que todos los mensajes deben pasar a través del enrutador que funciona como un *firewall*, todos los mensajes son revisados por el *firewall*.

Las reglas de un gateway de filtro de paquete deben ser como se representa en la Tabla 3.

Tabla 3 Reglas de gateway de filtración de paquetes

Accion	Dirección de destino	Puerto de destino	Dirección de fuente	Puerto de fuente
Denegar	Us.net		Enemy.net	
Permitir	Us.net		Friend.net	

Estas reglas le niegan cualquier cosa a us.net entrando de enemy.net en cualquiera de nuestros puertos o conexiones a la red. Además, le permiten cualquier cosa a us.net que entra de un friend.net en cualquier puerto. La sintaxis exacta varía y depende del enrutador en particular y su fabricante. A pesar del fabricante, el ingeniero de seguridad que se encuentra instalando el sistema debe explícitamente establecer todo lo que es permitido y lo que no es permitido. Esto no siempre es fácil de decidir o especificar.. Un usuario no autorizado puede conducir screen dumps y registrar keystrokes de usuarios internos, lo cual es una muy seria amenaza a la seguridad. Finalmente, cualquier loophole que se deja en el *firewalls* puede ser penetrado y vencer la seguridad y protección de su sistema.

Servicios de proxy

Un servicio proxy representa un servicio de cliente interno al mundo exterior. Mientras que está representando este servicio puede actuar un poco diferente para incrementar la seguridad. Hay dos tipos básicos de servicios proxy.

1.Servicios proxy gateway a nivel de aplicación y
2.Servicios proxy gateway a nivel de circuito

Un *firewall* de gateway a nivel de aplicación provee control de acceso reescribiendo todas las principales aplicaciones. Las nuevas aplicaciones residen en servidores centralizados que todos deben utilizar. A estos servidores se les refiere como servidores de guardia o *bastion hosts*, nombrados por castillos medievales altamente fortificados y son considerados los puntos críticos de seguridad. Estos servidores son frecuentemente dual-homed hosts (servidores que residen en más de una red). Las aplicaciones parecen funcionar en la misma forma que sus aplicaciones originales excepto que los loopholes de seguridad son retirados. Específicamente, las nuevas aplicaciones incluyen una agregada característica pequeña pero importante: la autentificación. Los *firewalls* de gateway de aplicación son excelentes complementos para gateways de filtro de paquetes.

Los gateways a nivel de circuito son similares a gateways a nivel de aplicación en que son diseñados para una aplicación individual. A diferencia de gateways a nivel de aplicación, son transparentes para los usuarios. Específicamente, una persona externa puede conectarse a una red a través de puertos TCP. En gateways a nivel de circuito, el *firewall* provee el puerto TCP y transmite los bytes de un lado para el otro, actuando como un cable y de ese modo completar el circuito sin interpretar nunca el protocolo de aplicación.

Ya que operan a un nivel más bajo, los gateways a nivel de circuito necesitan modificar al cliente para obtener la dirección del destino, el cual está de otro modo fácilmente disponible para gateways a nivel de aplicación. Frecuentemente, los clientes modificados se usan solo para conexiones externas. Toda la filtración se conduce basada solamente en fuente y destino sin información adicional de los comandos específicos. Además de transmitir los bytes, el cliente modificado y de ese modo el gateway a nivel de circuito conserva un registro del número de bytes transmitidos así como el destino de TCP. Si hay un sitio conocido que ha tenido un problema de seguridad, el administrador de sistema podría usar este registro para notificar a cualquiera en el sistema que desafortunadamente se ha conectado al sitio corrompido.

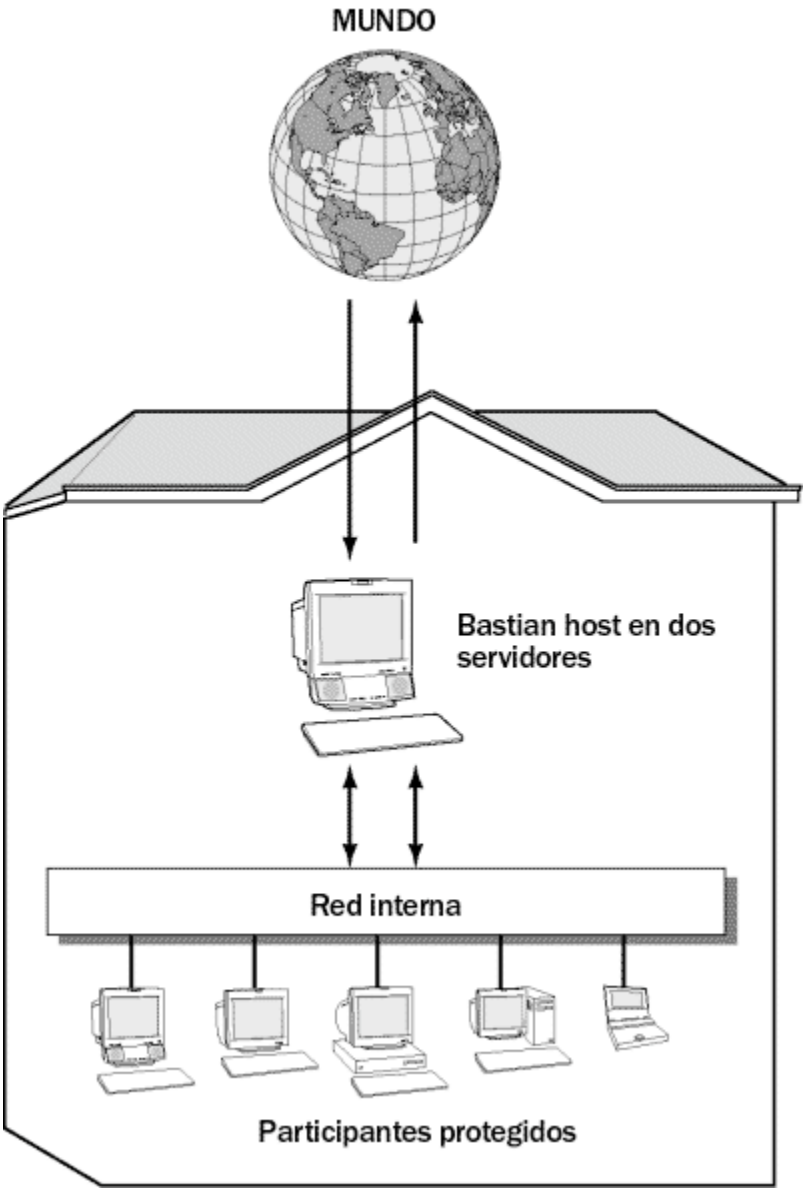
Arquitecturas de *firewall*

Ahora examinamos tres arquitecturas básicas de *firewall* que incorporan *firewalls* de filtración de paquetes y *firewalls* de servicios proxy.

Arquitectura *bastion host*

La arquitectura más simple es la de *bastion host*. Este diseño utiliza exclusivamente

un *bastion host* para proveer servicios proxy. Mientras que el servidor es capaz de enrutar información de una red a otra, esta característica del servidor no es recomendada ya que puede ser violada y finalmente usada para circundar su *firewall*. Todos los sistemas locales son considerados sistemas internos. Todos los sistemas que no son locales son considerados sistemas externos. El *bastion host* es un dual-homed host que reside entre los sistemas internos y externos. No se encuentra directamente en una u otra red pero opera como un gateway entre las redes. Todos los sistemas internos pueden comunicarse con el *bastion host* y todos los sistemas externos pueden comunicarse con el mismo *bastion host*. Los sistemas internos y externos no se pueden comunicar directamente uno con el otro pero se comunican teniendo los servicios de host proxy de parte de cada uno, como se representa en la Figura 3.6. Si el servidor recibe un paquete de información en su conexión externa con una dirección interna, ese paquete debe ser fraudulento. Esta arquitectura exhibe todas las debilidades de *firewalls* de servicio proxy, incluyendo las limitaciones de que servicios pueden proveer.



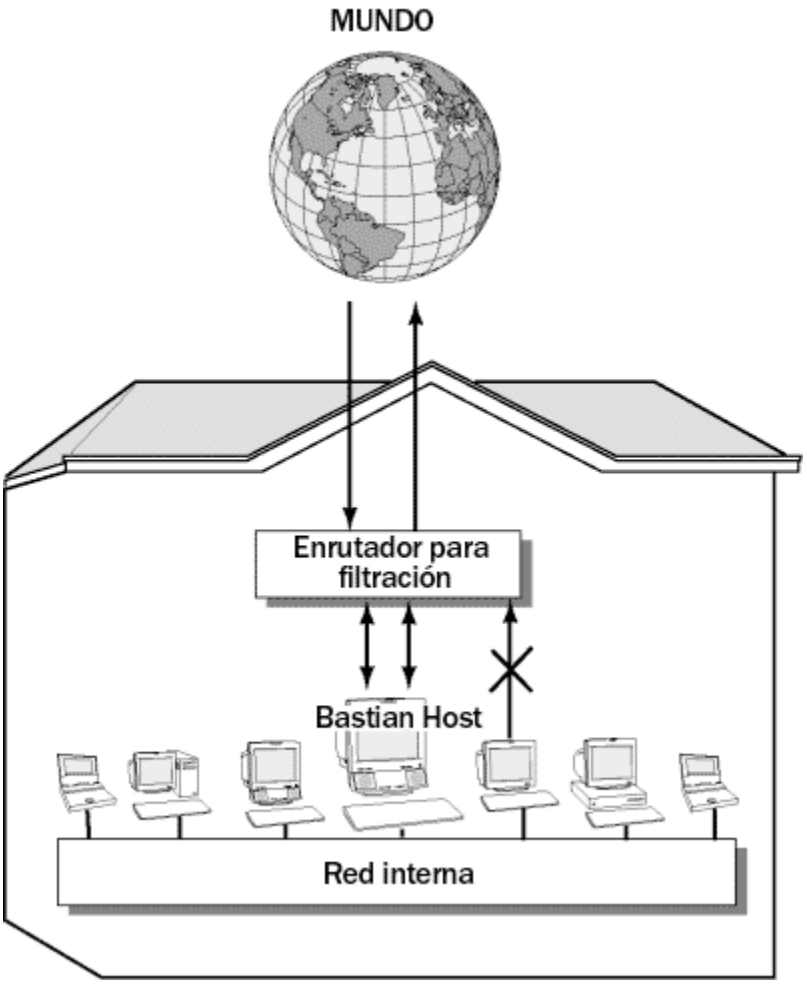
elaborado por :(“ Caballer, Xavier. (2004). Redes inalámbricas. URL; http:// http://www.hispasec.com/unaaldia.asp?id=1243”)

Figura 3.6 Arquitectura de *firewall bastion host*.

Arquitectura de filtración de servidor

La arquitectura de filtración de servidor utiliza un *bastion host* con servicios proxy y un enrutador actuando como una pantalla y proporcionando capacidades de filtración

de paquetes. A diferencia de la arquitectura previa, el *bastion host* reside en la red interna, como se representa en la Figura 3.7. Las capacidades de filtración de paquetes en el enrutador de filtración enrutan todo el tráfico externo permisible con destinos internos al *bastion host*. Además, el filtro de paquete puede ser configurado para permitir solo el acceso externo del *bastion host*. Si los servidores internos que no sean el *bastion host* se les niega el acceso al enrutador de filtración de paquetes, los servidores internos son obligados a usar los servicios proxy del *bastion host* para localizar servidores externos. De este modo, es probable que un sitio con fuertes requerimientos de seguridad no permita el acceso a servidores internos a la red externa directamente a través del *firewall* de filtración de paquetes.

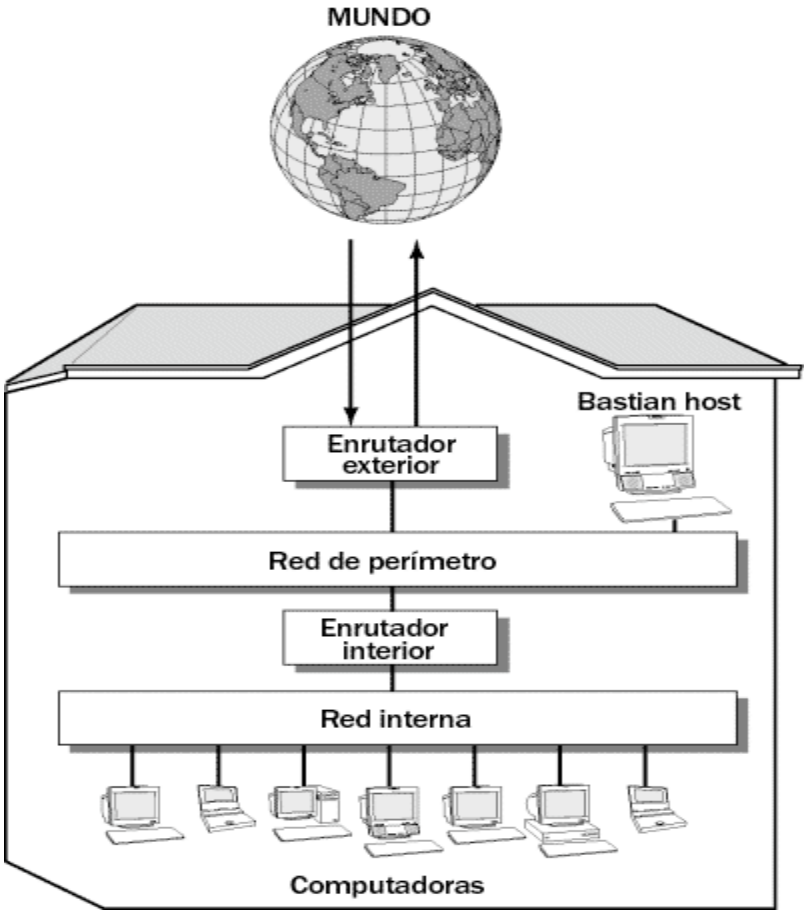


elaborado por :(“ Caballer, Xavier. (2004). Redes inalámbricas. URL; http:// http://www.hispasec.com/unaaldia.asp?id=1243”)

Figura 3.7 Arquitectura de *firewall* de filtración de servidor

Arquitectura subred de filtración

La más segura de las tres arquitecturas de *firewall* es la arquitectura subred de filtración. Esta arquitectura incluye dos *firewalls* de filtración de paquetes y un *firewall* de servicio proxy. El *firewall* de servicio proxy o *bastion host* está conectado a su propia red situada entre los dos *firewalls* de filtración de paquetes. Un *firewall* de filtración de paquetes conecta la subred del *bastion host* a la red externa. El otro *firewall* de filtración de paquetes conecta la subred del *bastion host* a la red interna, como se representa en la Figura 3.8. A la subred con acceso a la red externa se le refiere como una subred de filtración. Ya que es posible en la mayoría de las redes locales para que cualquier servidor en la red curiosee o vea todo el tráfico en la red, el principal beneficio de esta arquitectura es la falta de información solo interna en la subred de filtración. De ese modo, un intruso tendría que pasar al enrutador de filtración de paquetes, comprometer al *bastion host* y pasar al enrutador de filtración de paquetes interno para comprometer el control de acceso.



elaborado por :(“ Caballer, Xavier. (2004). Redes inalámbricas. URL; http:// http://www.hispasec.com/unaaldia.asp?id=1243”)

Figura 3.8 Arquitectura de *firewall* de filtración de subred

Seguridad y cifrado

A medida que las redes inalámbricas han ido ganando en popularidad, se hace más necesario fortalecer la seguridad de las mismas, es asombroso ver como más del 50% de empresas o personas que instalan su red inalámbrica no cifran la señal. Esto es equivalente a dejar abierta la puerta para que cualquier persona con un equipo portátil cercano a su organización pueda leer todo lo que pasa por la red por medio de un programa especial llamado "sniffer". Las formas básicas de cifrado para inalámbricas se conoce como: WEP (wired Equivalent Privacy) puede ser de de 64 o 128 bits. Este método de cifrado mejora sustancialmente la privacidad de la red pero no significa que no sea vulnerable, ya que un hacker con las herramientas y el tiempo suficiente podría descifrar la clave después de unas horas de análisis de las tramas. Por esto si la empresa maneja información muy sensible se recomienda implantar una VPN sobre la red inalámbrica de esta manera se agrega un mayor nivel de seguridad. El nuevo tipo de cifrado para las redes inalámbricas es conocido como WPA (Wireless Protected Access) y es un método de encripción para el 802.11 que utiliza una clave temporal (TKIP).

Como la clave es dinámica y cambia constantemente no puede ser descifrada fácilmente. Microsoft incluyó con Windows 2000 Server el servicio de IAS (Internet Autentication service) parte de su funcionalidad implementa el protocolo 802.1X que provee un medio para autenticar dispositivos que se conecten a una red LAN. Este estandar utiliza un servidor central de autenticación (con directorio activo) y valida a los usuarios tanto de la red inalámbrica como la red convencional.

Los procedimientos de seguridad de red deben cubrir todos los métodos de acceso a la red. Como una LAN inalámbrica conecta menos dispositivos en una zona geográfica más amplia, la mayor parte de las tareas de autorización se delegan a los sistemas operativos de otros dispositivos clientes, servidores u otros recursos de red.

Las tecnologías inalámbricas aumentan el riesgo de acceso no autorizado, ya que el usuario no necesita acceder a una conexión física en una pared o escritorio. Además, la zona de cobertura de esta tecnología puede extender el acceso a zonas que están incluso fuera de las paredes de la oficina corporativa.

La puesta a punto de un sistema de seguridad requiere un análisis previo de los riesgos que evalúe los costes en relación con otros factores indirectos como las pérdidas de ingresos o de negocio. Para asegurar la seguridad de la red cuando se usan tecnologías inalámbricas se sugieren las medidas siguientes:

a)Cerrar con llave la puerta de la sala de servidores o poner en marcha políticas de seguridad de alto nivel para impedir el robo, destrucción o modificación de los datos.

b) Usar hubs conmutadores en vez de hubs repetidores como medida de seguridad adicional.

c) Usar cifrado siempre que sea posible. Los equipos W-LAN 802.11b suelen contar con la opción de cifrado entre el dispositivo cliente y el punto de acceso.

d) Usar nombres de usuario, contraseñas o certificaciones digitales para asignar el nivel de uso autorizado y autenticar a los usuarios.

e) Instalar herramientas de detección de virus, daños e intrusión en la red.

Con estas sencillas medidas, la red será más segura y menos proclive a problemas y desastres que se pueden evitar.

Privacidad Equivalente a Cableado (WEP)

"La especificación 802.11b proporciona mecanismos de cifrado y capa de Control de Acceso a Medios (MAC), identificados con las siglas WEP, y que tienen el objetivo de proporcionar a las LAN inalámbricas un nivel de seguridad equivalente al de sus homólogas cableadas. WEP cifra los datos enviados mediante señal radio entre el dispositivo cliente (como una PC Card 802.11b) y un punto de acceso". ("Morguet Carlos V. (2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php")[Morguet Carlos V.,2003]

El sistema de cifrado WEP a 40 bits integrado en las WLANs 802.11b debe ser suficiente para casi todas las aplicaciones, pero la mayoría de los equipos pueden adquirirse con cifrado WEP a 128 bits. Además de la técnica de autenticación WEP 802.11 hay disponibles otras técnicas de control de acceso, incluyendo ESSID programada en cada punto de acceso para identificar el segmento de red conectado.

La certificación ISO X.509 es el estándar internacional en el que se basan la mayoría de las certificaciones digitales comerciales. Las certificaciones digitales representan la certificación de la clave pública de una persona, empresa u organización - y también se usan para certificar los privilegios y derechos del portador.

La certificación puede descargarse de un servidor a un cliente al realizarse la autenticación inicial, y se comprobará cada vez que el usuario intente acceder a ese servidor.

Las certificaciones digitales se usan para autenticar un servidor o un sitio Web, o identificar a un usuario. La certificación puede proporcionar también claves usadas para el cifrado. Así se garantizan la confidencialidad, integridad y seguridad de las comunicaciones y transacciones.

La red Privada Virtual (VPN) tiene las siguientes características:

- Los administradores de red pueden aumentar la cobertura de la red corporativa de una forma muy económica .
- Los usuarios remotos pueden acceder a la red corporativa con facilidad y seguridad
- Las corporaciones pueden comunicarse con sus socios comerciales con seguridad
- Las empresas pueden subcontratar la gestión de servidores y aplicaciones.

Los suministradores de servicios pueden aumentar su negocio proporcionando anchos de banda sensiblemente superiores y servicios de valor añadido. A medida que aumenta el número de trabajadores que viajan o trabajan a distancia, los servicios tradicionales de acceso remoto se han hecho más complicados y caros para poder satisfacer las necesidades de un personal cada vez más móvil y disperso.

Estas tendencias han alterado las estructuras de las redes tradicionales, y sobre todo la anteriormente muy nítida frontera entre una LAN privada y una WAN pública se ha hecho cada vez más difusa.

Para superar las limitaciones de los servicios WAN tradicionales se necesita una red de datos barata, robusta y que cubra todo el mundo, de modo que pueda acceder a ella cualquier persona en cualquier momento y desde cualquier lugar. Por supuesto, ya existen muchas e esas redes en la forma de la "nube" Internet y las redes troncales IP dedicadas que mantienen docenas de suministradores de servicios de red.

Internet ha sido el claro motor de una revolución basada en la disponibilidad generalizada de comunicaciones de datos ad-hoc a bajo coste. Pero a pesar de la revolución mundial en telecomunicaciones creada por Internet, éste sigue sin ser un medio adecuado para las comunicaciones comerciales, debido a sus problemas para garantizar la fiabilidad y calidad de servicio, capacidad de gestión de funcionamiento y seguridad.

Una VPN correctamente diseñada puede resolver estos problemas, proporcionando al usuario final una infraestructura de comunicaciones empresariales

mucho más potente a un coste mucho menor. Una VPN enlaza oficinas remotas a una red, proporcionando la capacidad para compartir datos e ideas eficazmente a lo largo y ancho de toda la empresa. Pueden añadirse con facilidad cortafuegos a una VPN para proporcionar un cifrado sólido que proporcione seguridad a los datos mientras viajan por Internet.

Las VPNs proporcionan acceso desde cualquier lugar desde donde se pueda acceder a Internet, y permite establecer comunicaciones amplias y flexibles con clientes, proveedores y socios comerciales a través de extranets.

Las VPNs proporcionan un sistema barato para ampliar la red corporativa hasta las oficinas más distantes, empleados que trabajan en casa, vendedores y socios comerciales. En vez de utilizar caras líneas dedicadas para acceder a las oficinas más distantes, las VPNs usan los servicios de red IP disponibles en todo el mundo, incluyendo Internet, y las redes de los proveedores de servicios IP. Cualquier sistema de ordenadores que esté configurado para trabajar con una red IP puede conectarse a una VPN sin que haga falta más modificación que la instalación del software remoto; además, se pueden crear VPNs entre corporaciones.

Capitulo 4 Recomendaciones para la seguridad en la transmisión de la información de los sistemas de la FES Acatlan, en redes inalámbricas

Dentro de la transmisión de información vía aire, el adecuado manejo y administración de los recursos que ofrece una infraestructura de tipo híbrida en cuanto a seguridad , debe de tomar en cuanto varios aspectos que aseguren un buen control y dominio de la información manejada dentro de la red, Para ello es necesario contar con el siguiente hardware y software empleado estratégicamente logrando aprovechar hasta el mínimo recurso que puede ofrecer, todo ello para garantizar el envío y recepción de datos de manera segura. Para poder llevarlo a cabo, hemos de conocer el uso, alcance y compatibilidad del hardware sugerido..

4.1 Estaciones y puntos de acceso

La infraestructura de un punto de acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son

1.- La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

2.- “La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.” (“Alarcon Jose M., (2004). Seguridad para redes inalámbricas. URL; http:// www.krasis.com”)

Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión. (esto no es posible en un sistema de estación-a-estación, en el cual no se aprovecharía el espectro y la eficiencia de poder, de un sistema basado en puntos de acceso)

La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda. En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10 Db en la recepción de transmisión de una estación sobre otra estación .

Estos 10 Db son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

Tomando en cuenta que la tecnología inalámbrica proporciona al usuario movilidad, opciones de instalación simples y flexibles, un costo reducido de adquisición (no genera gastos de cableado o mantenimiento) y la excelente adaptabilidad para soportar PC´s adicionales. Con 11 Mbps inalámbricos es ideal para usarla con cable módem, DSL o SOHO.

En la configuración inalámbrica típica un Punto de Acceso (transceiver) se conecta a una red de alambre con cableado estándar. El Acces Point soporta hasta 128 usuarios localizados a 25 metros de distancia del Access Point hasta un máximo de 457 metros. Los usuarios tienen acceso a la LAN vía la tarjeta inalámbrica de SMC en sus equipos portátiles o de escritorio. La tarjeta inalámbrica crea la interfase entre el Sistema Operativo de la red y el radio vía una antena (Access Point) como se muestra en la figura 4.1. Con un costo aproximado de USD$54.00. Para crecer la red inalámbrica LAN, solamente se necesita instalar más Access Point. En una configuración uno a uno no se requiere un Access Point, una tarjeta inalámbrica para cada equipo portátil o de escritorio es suficiente.

DWL-AP810 CLIENTE O ACCES POINT !!!!!!

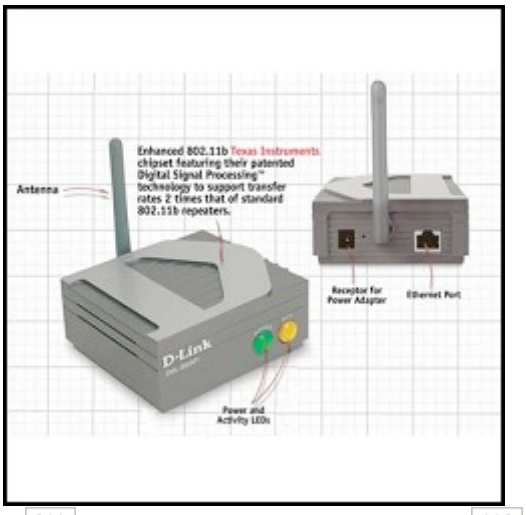


Fig. 4.1

Un adaptador basado en el estándar IEEE802.11b. Soporta comunicación inalámbrica a una velocidad de hasta 11 Mbps con un rango máximo de conexión de hasta 213 m. Soportando Windows/98/ME/NT/2000/XP esta tarjeta provee una sencilla configuración con una LAN inalámbrica existente.

Estas tarjetas generalmente tienen integrada una característica llamada fallback, la cual automáticamente se conecta a 1,2, 5.5 o 11 Mbps para proveer una mejor conexión. Para crear una conexión de red segura, esta tarjeta soporta encriptamiento WEP de 64-bit y 128-bit.

Sus Características y ventajas son:

- Conexión inalámbrica LAN de alta velocidad 802.11b.

-Soporta ad-Hoc (punto a punto) y modos de infraestructura.

-Encriptamiento WEP 64-bit/128-bit para asegurar transmisiones seguras de información a través de la red.

-Fallback automático que soporta una mejor conexión 5.5 o 11 Mbps

-Configuración plug & play – una instalación sencilla en segundos.

-Opera a una alta tasa de transmisión de datos hasta 11 Mbps y es interoperable con otros dispositivos como tarjetas PC inalámbricas, tarjetas inalámbricas PCI y adaptadores inalámbricos USB.

-Bajo consumo de energía y modo para ahorrar energía y usar el mínimo para conservar la batería de su PDA, Pocket PCs, Handheld PCs o notebooks Soporta la mayoría de sistemas operativos como Windows CE v3.0, Windows 98/NT/Me/2000/XP.

Compatibilidad

IEEE 802.11b

Un bridge inalámbrico está diseñado para conectar dos LANS o más, ubicados en diferentes edificios. Proporciona una alta tasa de transferencia de datos, y permite que las personas de el entorno puedan acceder a los recursos locales y remotos de la red.

Se conecta a la red troncal Ethernet mediante un conector RJ-45. El bride configurado como Bridge Master, también opera como un Access Point formando una clase de puente entre la LAN cableada y una o más estaciones de trabajo de PC inalámbricas móviles.

Características y ventajas:

- Alto rendimiento

LAN de 11 Mbps de alta transmisión de datos.

Rango máximo de cobertura – hasta 300 metros, dependiendo de las interferencias del entorno.

Banda de frecuencia 2.4 GHz no se requiere una licencia FCC DSSS (Direct Sequence Spread Spectrum) protege contra interferencias.

- Fácil para utilizar

Plug-and-play; nada que instalar ni configurar

- Compatibilidad

IEEE 802.3

IEEE 802.11b

Sistema operativo Windows 95/98/NT/2000

- Seguridad

Encriptamiento WEP 64 bits o 128 bits

4.2 Infraestructura de seguridad

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio. Los factores que permiten optimizar la capacidad de comunicación dentro de una área geográfica y del espectro de ancho de banda, son considerados más importantes que la forma de implementarse. Los diseñadores de sistemas únicamente pueden definir la utilización del espacio y del tiempo, y una aproximación de la eficiencia de la tecnología de transmisión por radio. Los diseños de alta eficiencia han sido evitados en sistemas de radio y redes porque su utilización no es muy obvia en cuanto a rapidez y conveniencia.

Uno de los aspectos más importantes de la eficiencia del tiempo es la asignación de frecuencia consolidada y el tráfico de cargas de usuarios no relacionados entre si. Por lo menos, el punto alto y el promedio de circulación de cada grupo deben de tener diferentes patrones; esto es muy difícil porque los canales incompartibles pueden ser vistos como viables, aunque su capacidad sea insuficiente para las necesidades máximas. Independientemente del rango, un conjunto de enlaces puede únicamente dar servicio a un fracción del área total. Para una cobertura total del área, se deben usar canales independientes, derivados por frecuencia, código o tiempo. No es fácil minimizar el número de canales independientes o conjunto de enlaces para una cobertura total. Mientras la distancia incrementa, se origina que la señal de radio disminuya, debido a la curvatura de la Tierra o a obstáculos físicos naturales existentes .Este diseño es muy utilizado en interferencia limitada. Existe una trayectoria normal cuando en el nivel de transferencia, de estaciones simultáneamente activas, no prevén la transferencia actual de datos. Para este tipo de diseño, los siguientes factores son importantes:

1.- Es necesaria una relación señal-interferencia, para una comunicación correcta.

2.- Se requiere de un margen expresado en estadísticas para generar esta relación, aún en niveles de señal variables

3.- La posición de las antenas que realizan la transmisión. La cual puede ser limitada por las estaciones y perfectamente controlada por puntos de acceso fijos.

4.- La función de la distancia para el nivel de la señal. Esta dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena de la terminales y los impedimentos naturales en la trayectoria.

Ahora se analizará el Factor de Reuso. El número del conjunto de canales requeridos es comúnmente llamado "Factor de Reuso" o "Valor N", para el sistema de planos celulares. “El sistema de planos celulares original, contempla 7 grupos de canales de comunicación y 21 grupos de canales de configuración basados en una estructura celular hexagonal. (Un patrón de un hexágono con 6 hexágonos alrededor, da el valor de 7, y un segundo anillo de 14 da el valor de 21.) Estos valores fueron calculados la Modulación de Indexamiento 2 FM, previendo un valor de captura de cerca de 12 dB y un margen de cerca de 6 dB. En los sistemas digitales el factor de Reuso es de 3 ó 4, ofreciendo menor captura y menor margen”. [Caballer, 2004]

- Factor de distancia

El promedio de inclinación de curva es reconocido por tener un exponente correspondiente a 35-40 dB/Decena para una extensión lejana y de propagación no óptica. Para distancias cortas el exponente es más cerca al espacio libre o 20 dB/Decena. El aislamiento de estaciones simultáneamente activas con antenas omni-direccionales pueden requerir factores de Reuso de 49 o más en espacio libre. La distancia de aislamiento trabaja muy bien con altos porcentajes de atenuación media. Depende de lo disperso del ambiente, la distancia de aislamiento en sistemas pequeños resulta ser en algunos casos la interferencia inesperada y por lo tanto una menor cobertura.

- Puntos de acceso

La infraestructura de un punto de acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son : la antena del repetidor debe estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa; la antena receptora debe ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión. (Esto no es posible en un sistema de estación-a-estación, en el cual no se aprovecharía el espectro y la eficiencia de poder, de un sistema basado en puntos de acceso)La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, si se ignoran estaciones que no tengan rutas de propagación bien definidas

entre si.Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. En cuanto al patrón horizontal este se puede incrementar de 1 hasta 24, depende del medio en que se propague la onda.

En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10 Db en la recepción de transmisión de una estación sobre otra estación .Estos 10 Db son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

Con un proyecto basado en Puntos de Acceso, la cobertura de cada punto de acceso es definible y puede ser instalado para que las paredes sean una ayuda en lugar de un obstáculo. Las estaciones reciben o transmiten activamente muy poco tiempo y una fracción de las estaciones asociadas, con un punto de acceso, están al final de una área de servicio; entonces el potencial de interferencia entre estaciones es mínimo comparado con las fallas en otros mecanismos de transmisión de gran escala. De lo anterior podemos definir dos beneficios del punto de acceso: 1.- El tamaño del grupo de Reuso puede ser pequeño (4 es el valor usado, y 2 es el deseado).

La operación asincrona de grupos de Reuso contiguos puede ser poca pérdida,y así permitir que el uso del tiempo de cada punto de acceso sea aprovechado totalmente. Estos detalles incrementan materialmente el uso del tiempo.

Respecto a la modulación de radio se puede decir que el espectro disponible es de 40 MHz, según el resultado de APPLE y 802.11 La frecuencia es "desvanecida" cuando en una segunda o tercera trayectoria, es incrementada o decrementada la amplitud de la señal. La distribución de probabilidad de este tipo de "desvanecimientos" se le denomina "rayleigh". El desvanecimiento rayleigh es el factor que reduce la eficiencia de uso del espectro con pocos canales de ancho de banda. Si es usada la señal de espectro expandido, la cual es 1 bit/símbolo, la segunda o tercera trayectoria van a causar un "Desvanecimiento" si la diferencia de la trayectoria es más pequeña que la mitad del intervalo del símbolo. Por ejemplo, una señal a 10 Mbs, necesita de 0.1 m seg. de tiempo para propagar la señal a 30 mts.

Las diferencias en distancias mayores de 5 mts. causan mayor interferencia entre símbolos que el causado por el "Desvanecimiento". Si el símbolo es dividido en 7 bits, el mecanismo ahora se aplicará a una séptima parte de 30 mts. (o sea, 4 metros aproximadamente), una distancia en la trayectoria mayor de 4 metros no es causa de "desvanecimiento" o de interferencia entre símbolos. El promedio de bits debe ser constante, en el espacio localizado en el espectro y el tipo de modulación seleccionado. El uso de ciertos símbolos codificados, proporcionaran una mejor resolución a la longitud de trayectoria. Un espectro expandido de 1 símbolo y cada símbolo con una longitud de 7,11,13, ...31 bits, permitirá una velocidad de 10 a 2 Mbs promedio. El código ortogonal permite incrementar los bits por símbolo, si son 8 códigos ortogonales en 31 partes y si se incluye la polaridad, entonces es posible enviar 4 partes por símbolo para incrementar la utilización del espacio. La canalización y señalización son

métodos que compiten entre sí por el uso de códigos en el espacio del espectro expandido. Algunos de los códigos de espacio pueden ser usados por la canalización para eliminar problemas de superposición.

El espectro expandido puede proporcionar una reducción del "Desvanecimiento" rayleigh, y una disminución en la interferencia a la señal para que el mensaje sea transmitido satisfactoriamente, lo cual significa que se reduce el factor de Reuso.

Para una comunicación directa entre estaciones de un grupo, cuando no existe la infraestructura, una frecuencia común debe ser alternada para transmisión y recepción. La activación, en la transmisión no controlada, por grupos independientes dentro de una área con infraestructura definida, puede reducir substancialmente la capacidad de organización del sistema.

Respecto a la eficiencia del tiempo se puede indicar que es importante para poder maximizar el servicio, al momento de diseñar la frecuencia en el espacio. El uso del tiempo está determinado por los protocolos y por los métodos de acceso que regularmente usen los canales de transmisión de la estación. Las características del método de acceso para que se considere que tiene un tiempo eficiente, pueden estar limitada por los métodos que sean utilizados. Algunas de estas características son:

1.- Después de completar una transmisión/ recepción, la comunicación debe estar disponible para su siguiente uso. a.- No debe de haber tiempos fijos entre la transmisión-recepción. b.- Rellenar la longitud de un mensaje para complementar el espacio, es desperdiciarlo.

2.- La densidad de distribución geográfica y tiempo irregular de la demanda del tráfico deben ser conocidas.

a.- Un factor de Reuso, es más eficiente por un uso secuencial del tiempo que por una división geográfica del área.

b.- Para la comunicación en una área, se debe de considerar la posibilidad de que en áreas cercanas existan otras comunicaciones.

c.- La dirección del tráfico desde y hacia la estación no es igual, el uso de un canal simple de transmisión y recepción da una ventaja en el uso del tiempo.

3.- Para tráfico abundante, se debe de tener una "lista de espera" en la que se manejen por prioridades: "El primero en llegar, es el primero en salir", además de poder modificar las prioridades.

4.- Establecer funciones para usar todo el ancho de banda del canal de comunicación, para que el tiempo que exista entre el comienzo de la transmisión y la disponibilidad de la comunicación, sea lo más corto posible.

5.- El uso de un "saludo inicial" minimiza tiempos perdidos, en el caso de que los paquetes transferidos no lleguen correctamente; cuando los paquetes traen consigo una descripción del servicio que requieren, hacen posible que se mejore su organización.

6.- La conexión para mensajes debe ser más eficiente que la selección, particularmente al primer intento, sin embargo la selección puede ser eficiente en un segundo intento cuando la lista de las estaciones a seleccionar sea corta. Para transacciones de tipo asincrona, es deseable completar la transacción inicial antes de comenzar la siguiente. Deben completarse en el menor tiempo posible. El tiempo requerido para una transacción de gran tamaño es un parámetro importante para el sistema, que afecta la capacidad del administrador de control para encontrar tiempos reservados con retardos, como hay un tiempo fijo permitido para la propagación, el siguiente paso debe comenzar cuando termina el actual. El control del tráfico de datos en ambas direcciones, se realiza en el administrador de control.

El limite de la longitud del paquete y su tiempo se refiere a que cuando el paquete es más pequeño, la proporción del tiempo usado al accesar el canal, es mayor, aunque la carga pueda ser pequeña para algunas funciones, la transferencia y descarga de archivos son mejor administrados cuando la longitud del paquete es de buen tamaño, para minimizar el tiempo de transferencia. En paquetes grandes, se incrementa la posibilidad de que el paquete tenga errores en el envío, en sistemas de radio el tamaño aproximado ideal es de 512 octetos o menos , un paquete con una longitud de 100-600 octetos puede permitir la salida oportuna de respuestas y datagramas prioritarios junto con los datagramas normales.

Es necesario proveer formas para dividir los paquetes en segmentos dentro de las redes inalámbricas. Para un protocolo propuesto, el promedio de mensajes transferidos, es mayor para el tráfico originado por el "saludo inicial", que el originado por el punto de acceso. En este promedio se incluyen campos de dirección de red y otras funciones que son agregadas por el protocolo usado y no por el sistema de radio. El mensaje más largo permitido para superar un retardo de acceso de 1.8. m seg. y un factor de Reuso de 4, utiliza menos de 600 m seg. Un mensaje de 600 octetos utiliza 400 m seg. a una velocidad de transmisión de 12 Mbs, los 200 m seg. que sobran pueden ser usados para solicitar requerimientos pendientes. El tiempo marcado para un grupo de Reuso de 4 puede ser de 2,400 m seg. Este tiempo total puede ser uniforme, entre grupos comunes y juntos, con 4 puntos de acceso; sin embargo la repartición del tiempo entre ellos será según la demanda. Las computadoras necesitan varios anchos de banda, lo cual depende del servicio a utilizar, transmisiones de datos, de video y voz de voz, etc.

La opción es, si:

1.- El medio físico puede multiplexar de tal manera que un paquete sea un conjunto de servicios.

2.- El tiempo y prioridad es reservado para el paquete y los paquetes relacionados con el, la parte alta de la capa MAC es multiplexada.

La capacidad de compartir el tiempo de estos dos tipos de servicios ha incrementado la ventaja de optimizar la frecuencia en el espacio y los requerimientos para armar un sistema.

Esta es una de las razones por las cuales conviene una red inalámbrica

Los Equipos necesarios se muestran a continuación en la figura 4.2

Acces Point

Va pegado a la red fisica y emite señal para vincular equipos inalámbricos

.

Tarjetas PC Card Para portatil

Tarjeta para equipo de escritorio (PCI)

Tarjeta externas USB Inalámbricas

Fig. 4.2

Los consumidores están demandando mayores capacidades multimedia - en sonido, datos, imágenes y video - en dispositivos móviles. Nuevas e innovadoras tecnologías permiten acceder a Internet, a una intranet corporativa o a su propia red doméstica desde cualquier lugar donde haya cobertura telefónica. Y en un futuro con dispositivos electrónicos más pequeños, baratos y potentes, la velocidad y la comodidad con la que se accederá a la información crecerán exponencialmente, es decir podremos acceder a imágenes de alta resolución en menor tiempo; otros beneficios pueden ser: Ahorro de tiempo, mayor rentabilidad, mejor comunicación, etc.

Según los analistas, el 60 por ciento de los productos electrónicos más importantes serán portátiles para el 2006 y muchos tendrán la capacidad e inclusive podrán llegar a requerir de conexiones con otros dispositivos. La nueva economía sin cables probablemente nos permitirá, con sólo hacer clic en un botón, tener disponibles nuestros historiales médicos y financieros. Pronto podremos elegir itinerarios y reservar viajes en tiempo real, ya en la carretera.

Tendremos sistemas celulares que estarán conectados a Internet permanentemente, videoteléfonos móviles y vídeo conferencias móviles. La tecnología inalámbrica está revolucionando las telecomunicaciones, ya que por medio de esta se simplifican y ahorran espacio, cables y lo que conlleva su instalación.; los nuevos dispositivos junto con la conectividad personal definirán un futuro sin cables - los cables, simplemente, no estarán permitidos.

Las tres categorías principales de tecnología inalámbrica son:

· Redes de área extensa - utilizadas para ofrecer servicio de telefonía móvil.

· Redes de área local o redes de área local sin cables - utilizadas para conectar entre sí varios ordenadores en un ambiente de oficina.

· Redes de área personal - utilizadas para crear una conexión entre dos o más dispositivos portátiles sin necesidad de cables o conectores.

La mayor revolución en las comunicaciones sin cables empezó con los teléfonos móviles. Los teléfonos móviles han sido el producto electrónico con más éxito de todos los tiempos, con más de 264 millones de unidades vendidas en 1999, un número que se espera que para el año 2005 se haya multiplicado por tres.

Para dar cobertura de transmisiones inalámbricas a un área geográfica determinada formando una red de área extensa (WAN), ésta se divide en zonas más pequeñas, denominadas células. Cada célula es la zona cubierta por una estación base radio de baja potencia con sus correspondientes antenas, y operando a frecuencias de radio individuales, que se repiten una y otra vez en otras células no adyacentes. Las llamadas realizadas en estas células se gestionan en las estaciones base o en conmutadores móviles. Estos últimos están conectados a bases de datos que hacen de interfaz entre la red inalámbrica y la red de telefonía cableada.

Cuando un teléfono móvil cruza los límites entre dos células, detecta que la señal de la célula que abandona es cada vez más débil, transfiriéndose automáticamente la llamada a la antena de la célula a la que se dirige cuando su señal sea la más potente.

Y como el sistema funciona con un nivel de potencia muy bajo, las frecuencias utilizadas en una célula determinada no producen ningún tipo de interferencia en células adyacentes.

Los usuarios que ocupan un área geográfica dada deben disputarse un número limitado de canales - y existen varios modos de dividir el espectro para proporcionar acceso de forma organizada:

El FDMA (Frequency Division Multiple Access) divide un espectro disponible en franjas no solapadas en la dimensión o dominio de la frecuencia. El FDMA es el modo más familiar de dividir un espectro y tradicionalmente ha sido utilizado por los sistemas análogicos.

El TDMA (Time Division Multiple Access) divide un espectro disponible en franjas no solapadas en la dimensión o dominio del tiempo. Los sistemas digitales son típicamente una combinación de FDMA y TDMA, donde la capacidad disponible se divide tanto en dimensiones de frecuencia como de tiempo, asignando a los usuarios canales de distintas frecuencias que utilizan en distintas franjas de tiempo.

El GSM (Global System for Mobile Communications) es un tipo de red digital inalámbrica TDMA con características de cifrado y usada ampliamente por toda Europa a 900 MHz.

El CDAM (Code Division Multiple Access) está basado en el concepto de espectro ensanchado, lo que significa que múltiples conversaciones comparten simultáneamente un espectro disponible y se distinguen entre sí mediante codificación en vez de usar canales de frecuencia o de tiempo.

Una compañía de telefonía inalámbrica que opera en un área geográfica definida ofrece este acceso WAN al usuario móvil en la forma de diversos planes y opciones de llamadas mensuales. Cuando sus abonados viajan fuera del área geográfica cubierta por la compañía, se les considera "en itinerancia" (roaming). Su compañía local transfiere el servicio a la compañía que opera esa área, con un coste de llamada mayor.

Existen dos tipos básicos de señales - analógica y digital. Una señal analógica puede tomar cualquier valor intermedio entre un máximo y un mínimo. Un ejemplo de señal analógica es la voz humana. Una señal digital no puede tomar cualquier valor, sino sólo un conjunto limitado de valores llamados símbolos, que pueden representar números o caracteres alfabéticos. Ejemplos de señal digital son un impulso de corriente en un cable o un impulso de luz en un cable de fibra óptica. Los sistemas inalámbricos tienden cada vez más hacia los sistemas digitales y el uso de formas avanzadas de modulación digital. Esto es debido a que la señal digital es más inmune al ruido y su manipulación o procesamiento es más sencillo que el de una señal analógica.

¿Y cuál es la diferencia entre teléfonos celulares y teléfonos PCS? Un teléfono celular utiliza transmisión analógica de onda corta o transmisión digital a través de una conexión sin cables. Un teléfono PCS es similar a un teléfono celular, pero utiliza exclusivamente transmisión digital, ofrece mayor movilidad y funciona a frecuencias más elevadas para conseguir una conexión de mayor calidad.

Los factores que contribuyen a incrementar el uso de WAN son:

· Cobertura de áreas mayores y precios más bajos.

· Integra llamadas locales y a larga distancia sin cargos extra por itinerancia.

· Mayor uso de servicios prepago.

· Mayor digitalización de las redes inalámbricas.

· Movilidad, comodidad y accesibilidad.

Redes de Área Local Tradicionales (LANs)

ARCN (Attached Resource Computer Network) o Arcnet es una tecnología LAN muy utilizada que se basa en un esquema token - bus y es la más barata de instalar, permitiendo usar cables más largos sin pérdida de ancho de banda.

Ethernet es la tecnología LAN más instalada y normalmente utiliza cable coaxial o tipos especiales de pares de cables trenzados para conseguir mayores velocidades de transmisión (el 10Base-T alcanza velocidades de hasta 10 Mbps, mientras que el Fast Ethernet o 100Base-T alcanza velocidades de hasta 100 Mbps).

FDDI (Fiber Distributed Data Interface) es un estándar para la transmisión de datos a través de líneas de fibra óptica que pueden extenderse hasta una distancia de 124 millas. Basado en el protocolo Token Ring, el FDDI puede cubrir grandes áreas geográficas y tiene capacidad para miles de usuarios.

Routers - Es un ordenador de propósito especial (o un paquete de software) que maneja la conexión entre dos o más redes y examina las direcciones destinatarias de los paquetes que pasan a través de ellas, decidiendo por cuál ruta enviarlos.

Los servidores son ordenadores que comparten sus recursos, como impresoras y archivos, con otros ordenadores pertenecientes a una LAN.

El conmutador es un dispositivo de red que selecciona un camino o un circuito para enviar una unidad de información a su próximo destino.

Token Ring - Es un sistema utilizado cuando varios ordenadores están conectados a una red configurada en forma de anillo o de estrella, para evitar la colisión de los datos de dos ordenadores si estos envían sus mensajes a la red al mismo tiempo.

Este es el segundo protocolo más utilizado para LANs.

Una red de área local (LAN) es un grupo de ordenadores y otros equipos relacionados que comparten una línea de comunicaciones y un servidor comunes dentro de un área geográfica relativamente limitada, como un edificio de oficinas.

Normalmente, el servidor contiene las aplicaciones y los controladores que cualquiera que se conecte a la LAN puede utilizar - un conjunto común de archivos y de información.

Las LAN pueden estar formadas por tan solo dos usuarios u ordenadores o por miles de ellos. Los usuarios también pueden compartir la misma impresora o escáner configurados para una LAN.

Implantar una LAN resulta caro debido al hardware y al cableado, sin embargo proporcionan un sistema eficaz para que un grupo de usuarios comparta un conjunto

de datos común y se comuniquen electrónicamente, sin necesidad de intercambiar disquetes y sin tener dudas sobre si están o no utilizando la versión más reciente de los archivos. Las actualizaciones de software se realizan una sola vez en el servidor, reduciendo gastos y tiempo de administración.

Redes de Área Local sin cables (WLANs) Una red de área local sin cables ofrece acceso sin cables a todos los recursos y servicios de una red corporativa (LAN) en un edificio o en todo un campus. Cuando los usuarios necesitan acceder a las bases de datos y a los servidores de la compañía mientras están en movimiento, la única solución que permite este acceso en tiempo real es la de la red inalámbrica.

Las WLANs proporcionan más libertad en el ambiente de trabajo para que los trabajadores móviles accedan a la red. A través de una red sin cables, los trabajadores pueden acceder a la información desde cualquier lugar de la compañía, es decir, independientemente del lugar en el que se situen ya sea -una sala de conferencias, la cafetería o incluso la oficina más apartada. Aunque están confinadas a ciertos límites geográficos, con las WLANs los usuarios no están limitados a unos determinados puntos de acceso a través de cables fijos para acceder a la red, sino que pueden hacerlo en cualquier momento y en cualquier lugar.

Esta libertad de movimientos ofrece a los usuarios numerosas ventajas:

· Acceso fácil y en tiempo real para realizar auditorías y consultas desde cualquier lugar.

· Acceso mejorado a la base de datos para supervisores itinerantes, como directores de cadenas de producción, auditores de almacén o arquitectos.

· Configuración de red simplificada con mínima implicación MIS para instalaciones en crecimiento o emplazamientos de acceso público, como aeropuertos, hoteles y centros de convenciones.

· Un acceso más rápido a la información del cliente para vendedores, servicios de mantenimiento y minoristas.

· Acceso independiente de la localización para administradores de redes, para facilitar el soporte y la resolución de problemas locales.

Redes de Área Personal.

Una red de área personal (PAN) es una red que existe dentro de un área relativamente pequeña, que conecta dispositivos electrónicos como ordenadores de sobremesa, impresoras, escáner, aparatos de fax, PDAs y ordenadores notebook - sin que sean necesarios cables ni conectores para que la información fluya entre ellos.

En el pasado, para conectar estos dispositivos era necesario el uso de gran número de cables, conectores y adaptadores. La existencia de diversas opciones de puerto incompatibles - USB, serie, paralelo - además de incómoda, tenía limitaciones y problemas de fiabilidad.

En marzo de 1998, se formó el WPAN Study Group con el propósito de investigar la necesidad de un estándar de redes sin cables para dispositivos en un área de funcionamiento personal. Justo dos meses después, en mayo de 1998, se formó el Bluetooth Spacial Interest Group (SIG) y, diez meses después, el WPAN Study Group se convirtió en el IEEE 802.15, el WPAN Working Group. El Bluetooth SIG, conducido ahora por 9 compañías promotoras - Ericsson, Nokia, Toshiba, IBM, Lucent, 3Com, Microsoft e Intel, continúa definiendo el estándar Bluetooth y promoviendo esta tecnología.

El estándar de comunicaciones sin cables WPAN se centra en los temas clave del bajo consumo (para alargar la vida de la batería de los productos portátiles), tamaño pequeño (para que sean más fáciles de transportar o incluso llevar encima) y costes bajos (para que estos productos sean lo más universales posible).

Las aplicaciones obvias de las WPANs se encuentran en la oficina, donde los dispositivos electrónicos de su espacio de trabajo estarán unidos por una red sin cables. Estos dispositivos pueden ser, por ejemplo, su ordenador de sobremesa o notebook, una impresora, su asistente personal digital, su teléfono celular, su busca y su estéreo portátil - y la lista continúa.

Limitadas actualmente sólo por la distancia geográfica, el futuro ofrece atractivas posibilidades para las WPANs, con aplicaciones dentro y alrededor de la oficina, la casa, el automóvil, el transporte público o cualquier emplazamiento.

Con la aparición de las nuevas tecnologías disponibles actualmente, como Bluetooth, las fronteras tradicionales entre WANs, LANs y PANs se han ido difuminando. Si todos los dispositivos disponen de tecnología Bluetooth, todo es posible.

No sólo se crean PANs entre dispositivos portátiles, se pueden crear también otras PANs que la enlazan con una WAN, LAN o WLAN ya existentes.

Por ejemplo, una persona acude a las oficinas de un cliente con un equipo de otros cinco asesores para celebrar una reunión. En la sala de reuniones su equipo crea una PAN y revisa al mismo tiempo una presentación PowerPoint en cinco notebook distintos y en un ordenador de sobremesa. También hay creada una PAN individual entre cada ordenador individual y sus periféricos - incluyendo ratones, teclados, aparatos de fax, escáners o impresoras.

Después de compartir un par de documentos con dos de los asesores, se da cuenta de que necesita acceder a la intranet de su cliente para conseguir información adicional.
Mientras usted crea otra PAN entre su notebook y la LAN del cliente para acceder a esa información, uno de sus colegas utiliza su teléfono móvil y su notebook para obtener una conexión con una WAN a través de su proveedor de red sin cables.

Después de comprobar su correo electrónico, vuelve a la reunión y crea otra PAN entre su notebook y la impresora para imprimir el correo electrónico nuevo. Después puede compartir esta información con cuatro de los otros cinco asesores a través de la PAN existente entre los PC y notebook de todos.

Podemos ver como las WANs, LANs y PANs trabajan conjuntamente de forma sencilla, compatible y sin cables - una potente posibilidad que nunca ha existido anteriormente.

A continuación veremos como se lleva a cabo la transmisión de tados internamente y referente a la seguridad que se tiene en la red inalámbrica establecida dentro de Acatlán asì como algunas medidas de seguridad que se pueden implementar para su mejora.

FES Acatlan

Actualmente la FES Acatlan cuenta con un centro de computo, el cual se encarga de administrar una red con topología en estrella en forma híbrida, contando solamente con algunos puntos de acceso situados estratégicamente en los edificios de Investigación , fundación UNAM y Centro Cultural, siendo de esta manera hasta cierto grado limitada la cobertura via inalámbrica y poco confiable debido a que solo cuenta con un firewalll y prioridades de entradas y salidas, lo que nos lleva de manera urgente a la realización de esta investigación mejorando en un alto porcentaje la transmisión de información segura dentro de la facultad, basándonos no solamente en el hardware mas competitivo en el mercado sino también empleando algoritmos lógicos que sin duda alguna mejorara la manipulación de información sobre todo en aquellas áreas donde solo deben de tener acceso personal autorizado.

A continuación se describe detalladamente con lo que cuenta la facultad y lo que se pretende implementar asi como sus mejoras.

- La transmisión de datos se lleva a cabo de manera interna, es decir el control de acceso se realiza por medio de firewall y se le conoce como primer filtro.

- El siguiente filtrado nos dirige a puertos permitidos y no permitidos. Dentro de los permitidos figuran el 80, 21,22,110,210,8080.

- La asignación de prioridades en cuanto a entradas desde Acatlan (de donde salen y de quien) se lleva a cabo por eliminación de poups.

- De manera general la red de la Fes Acatlán se administra vía wep con lo que se pretende mejorar la seguridad de transacción en cuanto a información.

- Maneja el protocolo TCP-IP, un protocolo muy conocido el cual se lleva a cabo por conexiones LAN y WAN. El NET BEUI y el IPX ISPX (protocolo de arquitectura Novell introduciodo en 1983 y que corre sobre cualquier plataforma).

- La velocidad que se maneja dentro de la red es de 100mps de manera interna. Y de 4 gigabytes de el edifico de mantenimiento al centro de computo (conmutador).

- LA topología empleada es la de estrella colapsado con anillo central.

Los planes contemplados a corto plazo referentes a la red y sus limitantes por parte de el centro de computo son los siguientes.

1.-Incremento de la seguridad (Proyecto de actualización referente a ínter conectividad de servicios)

2.- Proyecto TAC (sistema de asignación de casos mediante TRS (ticket request system)).

3.-SHCP

4.-Antivirus centralizado general.

5.- Directorio Activo Microsoft

6.-Renovación de infraestructura (compendio general de red y revisión)

Todo lo anterior contemplando la vulnerabilidad respecto a usuarios de manera directa.

Los aspectos considerados anteriormente demuestran claramente que se carece de una infraestructura apropiada y vulnerable, por lo tanto de una manipulación insegura de información. Todo esto nos lleva a el rediseño de la red de manera general dentro de lo cual se debe de tomar en cuenta los recursos por parte de la UNAM.

Ahora bien, dentro de lo que se pretende llevar a cabo dentro de Acatlán en cuanto a la red inalámbrica y la aplicación de la misma en los procesos escolares debemos de tener en cuenta las siguientes observaciones y mejoras en cuanto a esta seguridad.

La justificación que damos a la necesidad de redes inalámbricas es la siguiente:

“permite trabajar a gusto desde cualquier sitio, sin estar encerrado en una oficina o amarrado con un cable. Y de la manera mas segura en cuanto a el envio y recepción de información se refiere“

Esto podrá beneficiar sobre todo a las áreas como administración escolar, planeación etc., áreas en las cuales la información es confidencial y sumamente importante.

Ventajas de las redes inalámbricas.

Las ventajas y beneficios que nos ofrece la implementación y uso de una red inalámbrica son:

- Económicas: De acuerdo a comparaciones de costos que he visto, es mucho mas barato implementar una red inalámbrica que una cableada.
- Facilidad de instalación: Evita el tendido de cable estructurado. (tiempo y trabajo)
- Movilidad: Lo que se menciona al principio del articulo, la reubicación del equipo o el desplazamiento no afecta la conexión. (tomando en cuenta el alcance del punto de acceso).
- Es muy bien aceptada por los usuarios: Algo muy raro en el campo de la informática, ya que generalmente recibimos quejas y llamadas de los usuarios por problemas del cable, configuración o tarjetas de red. Con esta tecnología, puede disminuir si se asegura el correcto funcionamiento desde el inicio. (pero sin olvidar los problemas que pueden ser causados por interferencias)
- Incrementa la productividad: De igual manera, por medio de estadísticas, el personal se siente mas a gusto.

Principales aspectos de inseguridad en cuestion

Existe una serie de grupos que tienen un carácter supranacional, y que se extiende a través de su hábitat natural: Internet. A través de este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización. Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectara a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas.

Pero la situación ha cambiado: la ejecución del Plan Integral de Comunicaciones ha elevado tanto nuestras posibilidades que nos permite la integración en una única red de todos nuestros sistemas informáticos, con lo que conlleva a la hora de prestar servicios a los usuarios. Esto tiene su contrapartida, y es que el número de servicios que se ofrecen es directamente proporcional a los riesgos que se asumen, y sobre todo porque el primer enemigo al que habría que considerar podrían ser los propios usuarios.

De todas formas, el exceso de prudencia es contrario a la innovación y, por tanto, se están adoptando medidas que garanticen una cobertura suficiente: la adquisición de herramientas de software para la gestión de red, firewalls (cortafuegos, programas especializados en la protección de redes y sistemas), y software de auditoría; la elaboración de planes de seguridad tanto física como lógica y de las políticas correspondientes; y, por último, la mentalización de los usuarios para el correcto uso de los servicios que se prestan. De todas formas, la total seguridad nunca se podrá alcanzar, a menos que coloquemos los sistemas detrás de un muro infranqueable. Pero entonces nos encontraríamos con una red que es una auténtica autopista, pero por la que sólo circularían el correo electrónico y las páginas web.

Además, esto significa un incentivo para que los administradores de los sistemas y responsables de seguridad sean mejores en su trabajo, ya que cada ataque con éxito pone en evidencia nuestras deficiencias.

RESTRICCIONES LEGALES.

En algunos países existen muchas restricciones legales para el comercio electrónico, y esto impide la evolución del desarrollo de las aplicaciones y la implementación de software de seguridad para los negocios en línea.

Desgraciadamente, no sólo se enfrenta el problema técnico sino el legal porque cuando se utiliza una firma electrónica autorizada por las empresas involucradas en una transacción, por ejemplo, no se puede probar en un juicio que esta firma es auténtica. No existe una autoridad certificadora, éste es uno de los problemas más serios.

No se puede considerar que la seguridad sea cuestión de una sola cosa, ya que hay muchos elementos y soluciones en la infraestructura de informática de una red.

Por ejemplo, muchas de las claves en la criptología son fácilmente descifrables, debemos ver otras alternativas de tecnología de otros países de Europa, Israel, Rusia y no sólo en las soluciones americanas que presentan también muchas restricciones legales para su importación.

Algunas medidas para hacer frente al creciente problema de la falta de seguridad son: entre ellas la importancia de evaluar su vulnerabilidad interna y hacerse conscientes de que si bien existen muchas violaciones externas y muchas soluciones tecnológicas, existe un porcentaje muy alto de inseguridad interna como resultado de problemas organizacionales.

Esto enmarca la importancia de contar con políticas internas específicas que cuenten con el apoyo de los altos directivos, así como la existencia de un responsable en la seguridad interna cuyas decisiones de protección se realicen en función de problemáticas específicas y no sujetas a ajustes económicos.

Una vez realizado el estudio de las distintas áreas en que se divide la seguridad en Internet , nos concentraremos en los ataques de denegación de servicio distribuido o DOS/DDOS. Los motivos que llevan a la elección de este aspecto concreto de la seguridad son tan variados como importantes:

* Los ataques DOS/DDOS son los ataques más naturales en Internet. La conectividad universal existente permite atacar cualquier punto del mundo desde cualquier sitio. Esta característica intrínseca de Internet que le ha permitido, le permite y continuará permitiendo un enorme crecimiento es también su talón de Aquiles.

* Su presencia está a la orden del día con ataques directos contra servicios de Internet (como el famoso ataque a los servidores root del DNS) o incluso con virus como el MyDoom. De esta forma se prevé un aumento de la virulencia y efectividad en los DOS/DDOS.

* Actualmente no hay ninguna solución a este problema y las aportaciones de la comunidad científica no han pasado de los ámbitos académicos.
Tipos de inseguridades

Este es el talón de Aquiles de este tipo de redes. Si una red inalámbrica esta bien configurada nos podemos ahorrar muchos disgustos y estar mas tranquilos.

Las inseguridades de las redes inalámbricas radica en:

* Configuración del propio “servidor” (puntos de accesos).
* La “escucha” (pinchar la comunicación del envió de paquetes).
* “Portadoras” o pisarnos nuestro radio de onda (NO MUY COMÚN), mandan paquetes al aire, pero esta posibilidad es real.
* Nuestro sistema de encriptación (WEP, Wirelles Equivalent Privacy , el mas usado es de 128 Bits, pero depende el uso que le demos a nuestra red.

Nuestros datos son transmitidos como las ondas que recibimos en nuestra televisión o radio , si alguien tiene un receptor puede ver nuestros datos o si quiere estropearnos nuestro radio de transmisión.

COMO ASEGURAR UNA RED INALAMBRICA.

- Autentificación de Punto de Acceso y de los usuarios.

- Encriptación de datos WEP, Wirelles Equivalent Privacy.

Autentificación de puntos de acceso y de los usuarios.

Extensible Authentication Protocol (AP) o Extendido de Servicios (Extended Service Set - ESS) son formas de establecer una buena barrera de seguridad para poder identificar redes inalámbricas intrusas en una red o usuarios no permitidos. Utilizar estas opciones es muy recomendable ya que se establecen unos valores de seguridad usando la compatibilidad de nuestros propios productos. Si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro, también se determina si los dispositivos de control pertenecen a nuestra red o al conjunto Extendido de Servicios, el AP revisa si el identificador de ESS es idéntico al nuestro, si no lo son, aún siendo el mismo fabricante y mismo modelo de AP, no podrán participar en la red y no puede recibir ni enviar ningún paquete de datos.

Encriptación de datos WEP, Wirelles Equivalent Privacy.

WEP básicamente es la encriptación de nuestros datos o paquetes enviados por nuestra red, esto añade cierto grado de seguridad para evitar intrusos en nuestra red. Muchos usuarios son reacios al uso del WEP ya que se a demostrado que el cifrado puede ser ineficaz en algunas ocasiones, pero también puede ser un gran muro de seguridad si se realiza con ciertas reglas de uso.

Activamos la opción WEP Enabled.

Seleccionamos el tipo de encriptación que queremos usar, la codificación puede ser mas o menos segura dependiendo del tamaño, 64 Bits o 128 Bits.

Marcamos la casilla de 128 Bits esto aportara mayor seguridad a nuestra red, también podemos escoger entre una clave alfanumérica (13 caracteres) o Hexadecimal (26 caracteres 0-9/A-F) , no todos los modelos de redes inalámbricas soportan estas opciones. Si queremos una buena seguridad se recomienda usar un llave (Key 1 - Key 2 - Key 3 - Key 4) por día o por semana, cambiando las claves cada mes, esto aporta un grado de seguridad mayor y hacemos que nuestro futuro intruso tenga que trabajar mas en el intento de sacar o descodificar nuestros paquetes que circulan por nuestra red inalámbrica.

Estos consejos son para hacer una red inalámbrica un poco mas segura, las Wireless están avanzando cada día y se pueden añadir nuevas ideas de como mejorar nuestra seguridad.

Consejos de seguridad

Para que un intruso se pueda meter un nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar nuestra transmisión. Vamos a dar unos pequeños consejos para poder estar mas tranquilos con nuestra red inalámbrica.

1. Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.
2. Control de acceso seguro con autentificación bidireccional.
3. Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
4. Configuración WEP (muy importante) , la seguridad del cifrado de paquetes que se transmiten es fundamental en la redes inalámbricas, la codificación puede ser mas o menos segura dependiendo del tamaño de la clave creada y su nivel , la mas recomendable es de 128 Bits.
5. Crear varias claves WEP ,para el punto de acceso y los clientes y que varíen cada día.
6. Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.
7. Radio de transmisión o extensión de cobertura, este punto no es muy común en todo los modelos ,resulta mas caro, pero si se puede controlar el radio de transmisión al circulo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

Todos estos puntos son consejos, las redes inalámbricas están en pleno expansión y se pueden añadir ideas nuevas sobre una mejora de nuestra seguridad.
¿Y entonces cómo podemos asegurar nuestra red inalámbrica para que no entre nadie? Pues verdaderamente no podemos, si alguien quiere entrar entrará.
Lo más que podemos hacer es tomar las mayores medidas de seguridad posibles, redundando en:

1-Encriptación WEP de 128 usando claves no contiguas en el teclado y alternando mayúsculas y minúsculas y cambiarla regularmente.

2-Filtrando MACs.
3-Quitar dhcp.
4-Cambiar el SSID por defecto.

Un aspecto importante también es el echo del crecimiento en cuanto a equipos de escritorio así como lap-tops, lo mas usual dentro de la población, haciendo hincapié en los segundos, aquellos equipos portátiles con tecnología suficiente para conectarse vía aire a nuestra red , hecho que no debemos dejar de lado y a la ves tomarlo como un peligro potencial para nuestra red inalámbrica.

A continuación se muestra las estadísticas por parte del INEGI con base en el ultimo censo de población, lo cual nos puede dar una idea del crecimiento y posible aumente no solo de riesgo si no también de el aumento potencial de usuarios y saturación de la misma en un futuro no muy lejano, aspecto a considerar de notable importancia.

Indicador	**Valores (Por ciento)**		**Variación porcentual**
	2004	**2005**	
Como proporción del total de hogares			
Hogares con computadora	18.0	18.4	0.4
Hogares con conexión a Internet	8.7	9.0	0.3
Hogares con televisión	91.7	92.7	1.0
Hogares con televisión de paga	19.2	19.3	0.1
Hogares con servicio telefónico	59.9	64.1	4.2
Como proporción de la población de seis o más años de edad			
Usuarios de computadora	24.9	28.5	3.6
Usuarios de Internet	14.1	17.7	3.6
Como proporción del total de usuarios de computadora			
Usuarios de computadora que la usan como herramienta de apoyo escolar	53.0	60.0	7.0
Como proporción del total de usuarios de Internet			
Usuarios de Internet que han realizado transacciones vía Internet	6.4	5.8	-0.6

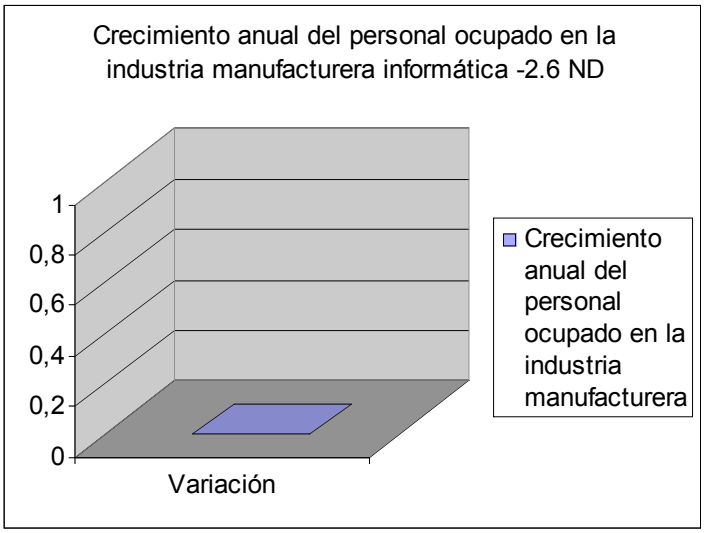
Usuarios de Internet que lo acceden desde fuera del hogar	61.5	68.3	6.8
Crecimiento anual del Producto Interno Bruto Informático	**17.4**	**ND**	**ND**
Crecimiento anual del personal ocupado en la industria manufacturera informática	**-2.6**	**ND**	**ND**

ND No disponible.

FUENTE: **INEGI.** *Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información en los Hogares.*

INEGI. *Sistema de Cuentas Nacionales de México. Producto Interno Bruto Trimestral 2002-2004.*

INEGI. Indicadores de la Encuesta Industrial Mensual por División y Clase de Actividad Económica, Banco de Información Económica.



La Topología en Estrella

Para los usos que requieren enlazar múltiples edificios, una topología en estrella puede ser la mejor opción. En esta topología, una unidad opera como estación base central, definiendo la secuencia de "polling" (interrogación secuencial). Las otras unidades se configuran como estaciones satélites (CPE, Customer Premises Equipment). Mediante el uso de protocolos para superar los problemas inherentes a los productos basados en la norma 802.11 por la existencia de transmisores ocultos. En el caso de Acatlan es la topología con la que se cuenta teniendo al centro de computo como polling y como estaciones satélites a los edificios de Investigación , fundación

UNAM y Centro Cultural.

Los usuarios a través de la red gozarán de un ancho de banda confiable, de una alta disponibilidad como nunca antes.

Se emplean sistemas de autenticación en la mayoría de las actividades diarias de trabajo. En las transacciones relacionadas con información personal o financiera, se debe mostrar una prueba de identidad.

La autenticación puede tomarse en dos contextos diferentes:

1.-Autenticación de Usuario. Es el proceso de determinar si una persona está autorizada para llevar a cabo una acción dada. Algunos sistemas de autenticación incluyen tanto identificación como autorización, mientras que otros solamente incluyen uno u otro.

De la misma manera, cuando se desea tener acceso a una porción privada de una red, normalmente se debe escribir el nombre de usuario (identificación) y la contraseña (autorización).

1. Autenticación de Datos. En los sistemas de procesamiento automatizado de datos, a menudo es imposible que alguien determine si los datos han sido modificados. Esta revisión llevaría demasiado tiempo si se tiene en cuenta la enorme cantidad de datos que manejan hoy en día las aplicaciones de procesamiento de datos.

Existen varios métodos para garantizar que los datos no hayan sido modificados intencionalmente o por error. Se trata de generar un código único asociado a determinados datos, de tal forma que si se modificaran los datos, dicho código sería diferente al original. Entre ellos podemos citar el chequeo de redundancia cíclica (CRC) y el chequeo de suma (Checksum). Estos dos métodos son adecuados para asegurar que no se hayan presentado modificaciones involuntarias.

Otro metodo para implementar es el VPN tunneling (túneles VPN (virtual private network -red privada virtual)) y acceso a redes de área local a través de puntos de entrada.. Sin embargo, las políticas no son suficientes para asegurar la red. Siempre habrá personas que obedecerán las normas y otras que no lo harán.por lo que se debera tomar medidas para dificultar extremadamente el acceso inalámbrico a la red para aquellos que no cumplen las normas.

Existen muchas formas de lograr este objetivo.Identificadores ESSID/SSID secretos.

El acceso a las redes inalámbricas 802,11b requiere un ID de servicio (ESSID/SSID) para acceder a la red inalámbrica. Funciona en forma similar a un grupo de trabajo bajo Windows.

Filtro de direcciones MAC

Toda tarjeta de red inalámbrica tiene un número de Control de Acceso a Medios (Media Access Control (MAC)) asignado de fábrica. Este número MAC, o dirección, es utilizado por la tarjeta para anunciarse en la red y ofrecer una forma de obtener información hacia y desde la tarjeta en los niveles de comunicaciones más bajos. Debido a que toda tarjeta tiene asignada una Dirección MAC única, esta dirección puede ser utilizada para otorgar o denegar el acceso de los usuarios a la red o área de impresión inalámbrica. Para aprovechar la seguridad de la dirección MAC y agregar un nivel adicional de control de acceso para la seguridad, se deberá configurar cada punto de acceso inalámbrico a fin de permitir el acceso a la red a las direcciones MAC específicas.

Con laptops robadas o tarjetas perdidas, aumenta el potencial para el acceso no autorizado utilizando solamente la Dirección MAC.

La sugerencia es contar con un sistema eficiente y efectivo para hacer un seguimiento de las direcciones MAC y sus dispositivos asociados. Una simple hoja de cálculo o base de datos es un buen comienzo y será más fácil de controlar si se implementa de inmediato.Virtual Private Network (VPN) (Red Privada Virtual)

Un método decisivo para proteger la red contra el acceso no autorizado es crear una red privada virtual que utilice encriptación. “En este tipo de redes la criptografía se presenta como una potente solución ante la debilidad que suponen las redes para la privacidad de la información que circula por ellas”.

Recordando, no obstante, que limitar el control de acceso a través de identificadores ESSID/SSID y direcciones MAC es sólo una de las facetas del sistema de seguridad general. Además de controlar el acceso, se necesita estar seguro de que la información que atraviesa las redes inalámbricas también esté encriptada.

En si, la implementación y uso de una red inalámbrica puede ser tan buena como sea su administración.

Administración de la seguridad

Una buena administración de una red inalámbrica comienza desde la conectividad en red sencilla, asequible y sin cables para las oficinas o lugares más pequeñas.

Este punto de acceso asequible y fácil de instalar constituye también una solución atractiva para crear redes domésticas y de pequeñas oficinas. Después de una instalación de tan solo unos minutos, los usuarios pueden empezar a acceder a los recursos de red, Internet y el correo electrónico; todo ello a velocidad estándar de Ethernet de 11 Mbps desde una distancia de hasta 100 metros (328 pies). Las características de rendimiento y fiabilidad integradas seleccionan automáticamente el mejor canal de radio y velocidad de conexión disponibles, manteniendo así las conexiones listas y abiertas. El punto de acceso emplea también seguridad mediante

encriptación WEP de 40/64 y 128 bits para proteger los datos en la LAN inalámbrica. Y ya que el punto de acceso dispone de certificación Wi-Fi, incluyendo switches y hubs para LAN, gateway routers firewalls, PC cards y adaptadores de red.

- Se instala en cuestión de minutos: el software del punto de acceso identifica y configura automáticamente los dispositivos de red, normalmente sin necesidad de configuración manual.

- Soporta hasta 128 usuarios simultáneos, a una distancia máxima de 100m.

- La encriptación WEP de 40/64 y 128 bits garantiza la privacidad de la transmisión inalámbrica.

- La función Clear Channel Select (selección de canal libre) escoge automáticamente el canal de radio con el menor tráfico para unas conexiones sin problemas.

- La función Dynamic Rate Shifting (cambio dinámico de velocidad) adapta automáticamente la mejor velocidad de conexión para responder a situaciones cambiantes de interferencia.

- Para redes de mayor tamaño, la función guardar y restaurar permite propagar los ajustes de configuración a todos los puntos de acceso en la red, simplificando y acelerando la configuración de LAN.

- La administración basada en “web” le permite configurar y administrar dispositivos de red desde cualquier lugar.

Las características integradas de seguridad, administración, actualización y fiabilidad hacen que resulte ideal para implementarse dentro de la FES Acatlan que se enfrente a crecientes necesidades de computación móvil como parte importante y fundamental de la UNAM.

Las herramientas de administración de red basadas en la Web hacen que la configuración y administración de la red resulte fácil, mientras que el soporte y supervisión permiten integrar la WLAN con su infraestructura cableada. La certificación Wi-Fi garantiza que el punto de acceso soportará todos los laptops, handhelds, PDAs, y otros dispostivos móviles inalámbricos compatibles.

- El estándar IEEE 802.11b de rendimiento para Ethernet inalámbrico a 11Mbps proporciona de tres a cuatro veces el ancho de banda de enlaces T1 (el caudal puede variar en función de la carga de tráfico en la red, de la distancia entre bridges, y del tipo de antena utilizado).

- Las múltiples opciones de antena garantizan la potencia de señal óptima para su situación.

- Los bridges inalámbricos tienen un precio competitivo y resultan económicos de operar, sin los costes recurrentes de equipos de cable o E1.

- El soporte de topología punto a punto o multipunto (one-to-one o one-to-many) proporciona una máxima flexibilidad al configurar redes entre edificios.

- El estándar 802.3af Power over Ethernet reduce los gastos de instalación de cable de alimentación y aumenta las opciones de ubicación, al utilizar un sencillo cable Ethernet para suministrar a la unidad tanto datos como alimentación.

- La función de cambio de velocidad dinámico ayuda a mantener las conexiones de red permanentemente disponibles al seleccionar la velocidad de conexión mejor adaptada a los casos radio inalámbrico.

- La encriptación WEP (Privacidad Equivalente al Cable) de 40 y 128 bits y la encriptación Dynamic Security Link (enlace dinámico de seguridad) de 128 bits protegen las transmisiones inalámbricas y de datos de red de posibles rupturas en la seguridad; la característica de tránsito VPN proporciona seguridad adicional.

- La administración fácil de usar y basada en la web permite a los administradores elegir entre gestionar todos los bridges de forma local desde cualquier punto de la subred, o bien hacerlo a distancia a través de Internet .

Con un buen bridge inalámbrico para grupos de trabajo se tendrá la oportunidad de conectar con la red inalámbrica cualquier dispositivo cableado de Ethernet, independientemente del sistema operativo que utilice y despreocuparse así de su configuración.

También tendrá la posibilidad de configurar los grupos de trabajo, conectando hasta cuatro dispositivos habilitados para Ethernet, que no dispongan de ranuras PCI (ordenadores, impresoras, escáneres, teléfonos y demás), mediante un solo bridge.

Utilice los sistemas de comunicaciones NBX®, de 3Com, para la implementación rápida y eficaz de redes de voz y datos completamente gestionadas.

- Mediante la utilización de un concentrador, podrá conectar hasta cuatro usuarios por bridge, obteniendo así unas conexiones inalámbricas muy asequibles.

- En la mayoría de casos, no se requiere ninguna configuración, simplificándose así este proceso.

- Es posible gestionar este bridge de forma remota mediante un navegador Web estándar, o bien mediante las herramientas de gestión SNMP.

- Auto Network Connect mantiene conectados a los usuarios en desplazamiento, con una opción de modo ad hoc o de infraestructura.

La certificación Wi-Fi ayuda a garantizar la interoperabilidad con productos de otros vendedores.

- Proporciona un acceso universal y completo a redes inalámbricas IEEE 802.11a, 802.11b, y 802.11g

- Soporta velocidades de hasta 54 Mbps, o 108 Mbps en modo turbo, sobre redes 802.11g o 802.11ª.

- La certificación Wi-Fi ayuda a garantizar que el PCI Adapter interoperará con los productos de otros fabricantes compatibles con WiFi.

- El control de acceso de red IEEE 802.1x y la autenticación EAP soportan las últimas y más efectivas técnicas de autenticación para deshacerse de los intrusos y simplificar la administración de red.

4.3 Accesos y autenticación

El objetivo de la autenticación de usuario es permitirle a una persona autorizada el acceso a un recurso físico, telemático o informático, previa verificación de que cumple con las condiciones exigidas para dicho acceso. Los métodos de autenticación de usuario existentes hoy en día son muy variados. Una forma de clasificarlos es de acuerdo a su relación con el usuario, así podemos diferenciar aquellos que se basan en datos conocidos por el usuario, los que requieren que el usuario lleve un dispositivo, y finalmente los métodos biométricos que se basan en rasgos físicos o en patrones de comportamiento del usuario. Es de anotar que en la práctica es común el uso de métodos combinados como por ejemplo datos conocidos por el usuario (PIN) y dispositivo (tarjeta), empleado para el acceso a cajeros automáticos.

Datos Conocidos por el Usuario

En esta categoría están las contraseñas usadas para el acceso a recursos informáticos, generalmente con un nombre de usuario asociado, y los PINs (Personal Identification Number) o NIPs (Número de Identificación Personal) para acceso a transacciones bancarias.

El principal problema de estos métodos de autenticación es que las claves para ser seguras deben ser complejas, y si son complejas, son difíciles de recordar para el usuario, quien fácilmente termina escribiendo el PIN en un papelito que mantendrá junto a la tarjeta bancaria, o claves de acceso en post-it pegados en la CPU o en la pantalla del PC.

Para eliminar estos problemas, se han creado sistemas de claves desechables, donde se le entrega al usuario una lista de claves, que se van usando una sola vez y de manera consecutiva. Obviamente, si otra persona obtiene dicha lista, puede lograr el acceso sin problema.

Dispositivos

Los dispositivos incluyen las tarjetas plásticas de banda magnética, las tarjetas inteligentes y los tokens o módulos de seguridad, entre otros.

Proporcionan una mayor seguridad que el método anterior, pero siempre y cuando sea el usuario autorizado quien las tenga en su poder.

Para evitar su uso por personas no autorizadas, estos dispositivos por lo general se usan en combinación con datos conocidos por el usuario, con lo cual se reduce así la posibilidad de acceso indebido si caen en manos equivocadas.

Métodos Biométricos

Los métodos anteriores verifican si un usuario está o no autorizado para tener acceso a un recurso pero no nos dicen nada relacionado con su identidad. Los métodos biométricos verifican la identidad del usuario, y con base en esta identificación proporcionan acceso a los recursos autorizados para ese usuario en particular. Podemos dividir los métodos biométricos en los que se basan en rasgos físicos del usuario y aquellos basados en patrones de comportamiento del usuario: rasgos físicos; escaneo de retina; reconocimiento de huella digital; reconocimiento de iris; reconocimiento de la cara; geometría de la mano; patrón de venas; análisis de DNA; comportamiento; análisis de firma; reconocimiento de voz y ritmo de uso del teclado

El escaneo de retina es de los métodos biométricos más antiguos. Se originó en investigaciones realizadas en los años 30. Hoy en día no es muy usado debido a que muchos consideran que es invasivo y que viola la privacidad: el usuario se debe situar el ojo a uno o dos centímetros del escáner y mirar una luz verde mientras se lee el patrón de vasos sanguíneos del fondo de su ojo. Además de lo molesto del procedimiento, este escaneo puede revelar datos adicionales a la identidad, como por ejemplo la existencia de un embarazo.

De los demás métodos, el sistema de reconocimiento de huellas digitales es el más popular en la actualidad, y le sigue el de reconocimiento de iris. Ambos métodos ofrecen un alto grado de seguridad.

Es posible que el análisis de DNA se use ampliamente en un futuro como método de autenticación, aunque hoy en día se emplea principalmente para investigaciones forenses y pruebas de paternidad.

Entre los métodos basados en patrones de comportamiento del usuario, el reconocimiento de voz es por ahora el menos confiable.

El método de reconocimiento de firma no sólo analiza la firma como tal sino la presión empleada en cada trazo de la misma. Los métodos biométricos tienden a generalizarse, usados en combinación con otros métodos de autenticación.

Red Segura

Se emplean sistemas de autenticación en la mayoría de las actividades diarias de negocios. En las transacciones relacionadas con información personal o financiera, se debe mostrar una prueba de identidad. Cuando deseamos cambiar un cheque en un banco, el cajero nos pide primero que le mostremos un documento de identidad antes de entregarnos el valor del cheque.

La autenticación puede tomarse en dos contextos diferentes:

1. Autenticación de Usuario. Es el proceso de determinar si una persona o una empresa está autorizada para llevar a cabo una acción dada. Algunos sistemas de autenticación incluyen tanto identificación como autorización, mientras que otros solamente incluyen uno u otro. Cuando se inserta una tarjeta débito en un ATM, se pide que ingrese un Número de Identificación Personal (conocido como PIN o NIP). El NIP le indica al Cajero Automático que está autorizado para llevar a cabo la transacción solicitada.

De la misma manera, cuando se desea tener acceso a una porción privada de una red, normalmente se debe escribir el nombre de usuario (identificación) y la contraseña (autorización).

2. Autenticación de Datos. En los sistemas de procesamiento automatizado de datos, a menudo es imposible que alguien determine si los datos han sido modificados. Esta revisión llevaría demasiado tiempo si se tiene en cuenta la enorme cantidad de datos que manejan hoy en día las aplicaciones de procesamiento de datos.

Existen varios métodos para garantizar que los datos no hayan sido modificados intencionalmente o por error. Se trata de generar un código único asociado a determinados datos, de tal forma que si se modificaran los datos, dicho código sería diferente al original. Entre ellos podemos citar el chequeo de redundancia cíclica (CRC) y el chequeo de suma (Checksum). Estos dos métodos son adecuados para asegurar que no se hayan presentado modificaciones involuntarias, sin embargo no evitan modificaciones intencionales, ya que el atacante podría generar el código correcto después de modificar los datos. Una manera de proteger los datos contra modificaciones no autorizadas es mediante un Algoritmo de Autenticación de Datos (DAA) criptográfico.

Las conexiones de red siempre presentan potencial para violaciones de seguridad dentro de la red y los entornos inalámbricos plantean nuevos desafíos que los entornos cableados han minimizado. Si bien una red de cable tiene un número finito de entradas a la red, un punto de acceso inalámbrico presta servicio a cualquier dispositivo dentro del alcance efectivo de la tecnología. Con tecnologías tales como IrDA o Bluetooth, se puede limitar la proximidad física para evitar cualquier acceso aislado a dispositivos de la red corporativa. Sin embargo, las tecnologías inalámbricas que ofrecen conectividad de largo alcance, tal como 802,11b, plantean diferentes problemas de seguridad porque, en general, no pueden contenerse dentro de los límites del espacio de la oficina.

Las políticas de seguridad de las grandes compañías incluyen el acceso a la red corporativa . En general, estas políticas abarcan temas como acceso telefónico, acceso a Internet, VPN tunneling (túneles VPN (virtual private network -red privada virtual)) y acceso a redes de área local a través de puntos de entrada. No obstante, es posible que el acceso inalámbrico a la red corporativa no esté incluido dada su reciente aparición en la escena de las conexiones de red. Es posible que tu compañía necesite reformar las políticas de seguridad a fin de incluir una cláusula para controlar el acceso a un área de impresión inalámbrica insegura por parte de personas ajenas a la compañía. Sin embargo, las políticas no son suficientes para asegurar la red. Siempre habrá personas que obedecerán las normas y otras que no lo harán. Deberás tomar medidas para dificultar extremadamente el acceso inalámbrico a la red para aquellos que no cumplen las normas. Existen muchas formas de lograr este objetivo.Identificadores ESSID/SSID secretos

El acceso a las redes inalámbricas 802,11b requiere un ID de servicio (ESSID/SSID) para acceder a la red inalámbrica. Funciona en forma similar a un grupo de trabajo bajo Windows. Cuando seintenta acceder a una red inalámbrica, se necesita tener un ID de servicio específico para participar en esa red. Aunque esto parezca una contraseña, en realidad, es una forma de hacer un seguimiento del punto de acceso que una tarjeta debería estar utilizando en casos donde existen puntos de acceso inalámbricos superpuestos. En realidad, existen programas "snoop" (espías) que estarán atentos al SSID que está siendo utilizado a fin de que nadie pueda tener acceso a la red inalámbrica con ese ID. Al mantener la seguridad de los identificadores ESSID/SSID (de la mejor manera posible a pesar de los programas snoop), se logrará un mayor control de las personas con acceso a la red y mantener alejados a los visitantes indeseados .

Filtro de direcciones MAC

Toda tarjeta de red inalámbrica tiene un número de Control de Acceso a Medios (Media Access Control (MAC)) asignado de fábrica. Este número MAC, o dirección, es utilizado por la tarjeta para anunciarse en la red y ofrecer una forma de obtener información hacia y desde la tarjeta en los niveles de comunicaciones más bajos. Debido a que toda tarjeta tiene asignada una Dirección MAC única, esta dirección puede ser utilizada para otorgar o denegar el acceso de los usuarios a la red o área de impresión inalámbrica. Para aprovechar la seguridad de la dirección MAC y agregar un nivel adicional de control de acceso para la seguridad, se deberá configurar cada punto de acceso inalámbrico a fin de permitir el acceso a la red a las direcciones MAC específicas. Por default, se denegará el acceso a la red a toda persona no incluida en esa lista. Si bien suena como una forma fantástica de controlar el acceso a la red, puede volverse incontrolable rápidamente. Es posible que las compañías con pocas laptops, PDA o demás dispositivos inalámbricos controlen la lista durante un tiempo, pero, eventualmente, será difícil mantener un registro de los dispositivos con permiso legítimo para acceder a la red. Con laptops robadas o tarjetas perdidas, aumenta el potencial para el acceso no autorizado utilizando solamente la Dirección MAC.

La sugerencia es contar con un sistema eficiente y efectivo para hacer un seguimiento de las direcciones MAC y sus dispositivos asociados. Una simple hoja de cálculo o base de datos es un buen comienzo y será más fácil de controlar si se implementa de inmediato.Virtual Private Network (VPN) (Red Privada Virtual).

Un método decisivo para proteger la red contra el acceso no autorizado es crear una red privada virtual que utilice encriptación. “En este tipo de redes la criptografía se presenta como una potente solución ante la debilidad que suponen las redes para la privacidad de la información que circula por ellas”. [Caballero, 1999] Crear un "túnel" entre el cliente y el recurso de red se puede implementar para proteger los datos contra ojos curiosos, pero no evita el acceso a la red inalámbrica o área de impresión inalámbrica. Si se tienen datos sumamente importantes, es posible que se prefiera este método de acceso para mantener la seguridad de los datos durante su transmisión desde la laptop de un cliente a un servidor o impresora en red.

Recordando, no obstante, que limitar el control de acceso a través de identificadores ESSID/SSID y direcciones MAC es sólo una de las facetas del sistema de seguridad general. Además de controlar el acceso, se necesita estar seguro de que la información que atraviesa las redes inalámbricas también esté encriptada.

Por lo tanto la Topología en Estrella.Para los usos que requieren enlazar múltiples edificios, sera la mejor opción. En esta topología, una unidad de SPEEDLAN 9000 opera como estación base central, definiendo la secuencia de "polling" (interrogación secuencial).

Las otras unidades se configuran como estaciones satélites (CPE, Customer Premises Equipment).

Altamente escalable, cada estación base puede servir hasta 100 edificios remotos a la vez, y puede sobre-suscribirse hasta niveles de 5 a 1 para aplicaciones ISP. Una vez que una red en estrella, la estación base supervisa actividad de cada CPE y optimiza el ancho de banda para cada estación remota. Con la asignación dinámica del ancho de banda, los CPE remotos con una carga de tráfico densa se interrogan más con frecuencia que CPE con un tráfico ligero. Los usuarios a través de la red gozarán de un ancho de banda confiable, de una alta disponibilidad como nunca antes.

Con la topología de estrella, las aplicaciones ubicadas en las áreas académicas, inaccesibles hasta ahora por vía inalámbrica, son fácilmente accesibles. A diferencia de los sistemas basados en topología punto a punto o multipunto, no se requiere un estudio de línea de vista para determinar si la estación base puede ser vista desde la ubicación requerida. Basta con que se “ vea ” cualquier otra de las unidades y listo, estaremos conectados. Y, como una ventaja asociada, cada nuevo edificio agregado a una red le amplía su capacidad de conectar aún más edificios. El tiempo de instalación por el edificio se puede reducir a una hora o menos, disminuyendo dramáticamente los costos de instalación.

Con su combinación única de opciones de configuración, la red inlalambrica proporciona la flexibilidad, escalabilidad y poder que se requieren asi como la capacidad para soportar los multiples proyectos que se implementarán a futuro y el rediseño próximo a la red. Otro aspecto de vital importancia es la vulnerabilidad de la misma en cuanto a usuarios y gestion de los mismos asi como lo que respecta a el

factor económico, logrando asi cubrir las necesidades dentro de la FESA (antes ENEP Acatlan). Finalmente logrando interconectar edificios de manera inalámbrica y no compleja, todo ello al alcance de la Universidad Nacional Autonoma de México.

CONCLUSIONES

La mayoría de las personas sienten seguridad cuando están utilizando una red alámbrica, pero tan pronto como los datos comienzan a viajar a través del “aire”, se preocupan. Después de todo, lo que se piensa es, la red alámbrica se encuentra dentro de sus instalaciones, y eso hace pensar que ya tiene algún elemento extra de seguridad. La verdad, es que cualquier red, incluida una red alámbrica, esta sujeta a potenciales riesgos de seguridad:

· Ataques desde dentro del grupo de usuarios de la red.

· Acceso no autorizado.

· Fuga de información hacia fuera de la compañía.

Los primeros pasos hacia las redes inalámbricas ya se están dando tanto en las compañías interesadas en proporcionar los servicios como en los potenciales usuarios. Las redes de comunicación están empezando a evolucionar hacia aquellos estándares universales capaces de soportar todos los requerimientos de comunicaciones. Se trata quizás de la única alternativa viable a los actuales sistemas de transmisión y conmutación para soportar cualquier tipo de trafico y que, a la vez, garantice una oferta de servicios avanzados , flexibles y sobre todo seguros de manera competitiva.

En este caso lo aplicable y funcional que puede ser para la FES Acatlán tomando como punto de partida su seguridad y lo factible que es esta, así como sus características principales, entre ellas destacables su alto rendimiento en transmisión de datos tratando de superar su actual velocidad (100 mbps), su rango máximo de cobertura, banda de frecuencia y configuración. Compatibilidad IEEE 802.3 IEEE 802.11b y sistemas operativos bajo los que corre, así como la seguridad q ofrece en cuanto a encriptación WEP 64 bits o 128 bits contra la actual, ya que conforme avanza la tecnología, también lo hacen las amenazas, en este caso y como aspecto fundamental la información que se transmite vía aire.

Las buenas noticias es que hay formas de combatir estas amenazas como se observo y explico en el capitulo 4 de acuerdo a las necesidades de la FES Acatlan.(firewalls, software de monitoreo, políticas de uso, etc.) para redes tanto alámbricas como inalámbricas y, de hecho, los segmentos de redes inalámbricas incluyen algunas funciones de seguridad incluidas que tal vez no tengamos consideradas.

De l objetivo planteado inicialmente se podrá lograr un 70 %de efectividad tomando en cuenta la infraestructura para adquirir y con la que se cuenta actualmente.

En cuanto a estas otras ventajas adicionales con las que cuenta son:

1. Facilidad de Instalación. La administración por web es sencilla y la instalación de los equipos y de las tarjetas también es muy sencilla.

2. Movilidad. Las redes tienen un rango de aproximadamente 10 metros alrededor de donde esta ubicado el punto de acceso. Sin embargo, las paredes disminuyen la intensidad de la señal.

3. Facilidad de configuración para el usuario. La persona que se va a conectar a la red solo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red esta abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente.

El análisis así como las recomendaciones de aquellas medidas de seguridad nos garantizan la privacidad y protección de los sistemas de la FES acatlan transmitidas a través de una red con estas características.

Todas estas ventajas y medidas de seguridad que en este trabajo se ofrecen son parte de la tecnología emergente para lograr un acceso seguro a la red,logrando un mayor grado de confiabilidad en cuanto al manejo de información, mayor cobertura a nivel facultad y un facil acceso a la misma. a su vez que estará siendo utilizada para llegar a aquellos lugares remotos sin suficiente capital cubriendo aquellas necesidades demandadas por parte de la comunidad de la FES Acatlán.

De esta manera además de los edificios que ya cuentan con esta tecnología (Tienda UNAM , Centro Cultural, Fundación UNAM, Investigación) podrán gozar de los beneficios y seguridad que ofrece una red inalámbrica.

Por lo tanto la FES Acatlán debe luchar por contar con la más nueva tecnología y poder apoyarse en ella de manera segura. Concluyendo así que las redes inalámbricas no son solo el futuro de la transmisión segura de datos, son el presente.

GLOSARIO.

A

Acceso - Servicio entre un punto "A" y un punto "B" que utiliza medios de comunicación tales como radio, par metálico, fibra óptica o satélite.

Acceso dedicado - Servicio entre dos puntos utilizado por un único cliente.

ACCOUNT(CUENTA).- Es el nombre con que se describe la autorización de una persona para acceder a Internet. Todo el que utilice esta red debe poseer una cuenta personal.

ADN. Se refiere, por lo general, a líneas dedicadas de 56Kbps., comunes en EEUU. En cambio, en España tiene un equivalente que serian las líneas de 64Kbps.

adsl (asymetric digital subscriber live). Este tipo de tecnología permite la transferencia de archivos a mayor velocidad que lo normal (de 27 a 160 veces mas rápido que un módem de 56K), usando una línea telefónica común.

alt. Nombre con el que se denomina a un tipo de newsgroup.

ANCHO DE BANDA (bandwidth).- Es la capacidad para transmitir información que posee cualquier tecnología de la comunicación (usualmente medida en bits por segundo), que puede ser transferida por Internet o cualquier red local. Es la cantidad de información que se puede transmitir en una unidad de tiempo.

anonymous ftp (ftp anonimo).- Es el método usado para loguearse dentro de un sitio con un seudónimo o nombre anónimo, para dar a conocer archivos con acceso publico.

Api (aplication program interface).- Es el conjunto de rutinas del sistema que se pueden usar en un programa para las gestión de entrada/salida, gestión de ficheros, etc.

ARPANET .-Fue una gran red, fundada por ARPA (Advanced Research Projects Agency – Dependencia de Proyectos de Investigación Avanzada). Funciono desde 1969 hasta 1990, como base de las primeras investigaciones sobre redes y como uno de los pilares fundamentales durante el desarrollo de Internet.

B

BACKBONE.- Literalmente significa "esqueleto" en ingles. Es el cableado a nivel superior de Internet. Conecta entre si las redes regionales, para formar así redes nacionales.

Back to Back .-Son equipos utilizados cuando se desea repetir la señal enviada por un equipo cuando la distancia a ser recorrida es mayor de lo recomendable. Realiza una ampliación en la señal debilitada, reforzándola para que llegue al punto de destino.

Backbone - Es una red de alta capacidad que conecta redes de capacidad menor. El backbone normalmente emplea los medios de transmisión más rápidos de la red y también puede cubrir distancias mayores.

baud.- Es un tipo de medida a través de la cual se mide la velocidad de un módem. Este envía y recibe información en bits. Numero de bits de información por segundo. Un baud es un símbolo, y ese símbolo esta formado por un grupo de bits (P ej: si un baud equivale a ocho bits, en ese caso, un baud será lo mismo que 8 bits)

bbs (bulletin board system).- Se usa con el fin de permitirle a los usuarios que se comuniquen enviando y recibiendo información de la central (servidor). Con este sistema, los usuarios se puede comunicar sin tener que estar conectados en forma simultanea.

.bit (binary digit).- Es la unidad mas chica con la que se mide el tamaño de cualquier tipo de dato informático. Puede tener dos estados, 0 y 1.

bps (bits per second).- Es el numero de bits transmitidos en un segundo.

Bridges .- Dispositivo que conecta a dos segmentos de la red, los cuales pueden ser de tipos semejantes o no, por ejemplo, Ethernet y Token Ring.

BROWSER.- Termino aplicado a los programas que permiten al usuario acceder al www.

bug .- Es un malfuncionamiento, un error o un desperfecto en el software. Esto perjudica al sistema provocándole interferencias en la maquina.

Byte.- Es la unidad con la que se miden los datos de carácter simple. Equivale a 8 bits cada un byte de información.

C

Cable módem - Módem usado para conectar una computadora a un sistema de TV a cable que ofrece servicios de red.

CABLEADO.- Es la unión entre el servidor y sus clientes-usuarios. Existen tres tipos de cableado; mediante cable coaxil, fibra óptica o par trenzado.

Caudal.- Cantidad de ocupación en un ancho de banda. En una línea de 1Mbps puede haber un caudal de 256 Kbps, con lo que los 768 Kbps restantes, del ancho de banda pueden permanecer desocupados.

CCIIT (INTERNATIONAL CONSULTATIVE COMMITEE ON TELEGRAPHY AND TELEPHONY).- Es el Comité Consultivo de Telegrafía y Telefonía. Organización que establece estándares internacionales sobre comunicaciones.

Cliente.- Es una aplicación especializada en un tipo determinado de conexión (telnet, ftp, gopher, www, etc) que soporta un protocolo especifico. También es un sistema o

proceso que solicita a otro un servicio determinado. (Una estación de trabajo que solicita el contenido de un fichero a un servidor de ficheros, es un cliente de este servidor)

Cobertura .- Área atendida por el Backbone de una red de telecomunicaciones.

Colocation (Co-locación) .- El alquiler de espacio físico de rack (abierto, cerrado o jaula), ancho de la banda y conectividad de la red en un Internet Data Center. Cookies – Archivo de texto especial que registra sus preferencias cuando usted utiliza un determinado sitio; también es capaz de almacenar las informaciones suministradas por usted en formularios en línea.

CONEXION dial-up.- Es la conexión que se da entre el módem de una maquina y el servidor mediante una línea telefónica.

Conexión redundante.- Conexión alternativa que permite mantener la comunicación en caso de que el primer dispositivo tenga deficiencias en su funcionamiento.

CONFIGURACION.- Es la forma en que se ordenan y organizan los datos, y el software, de una computadora, para que esta funcione en forma correcta y sincronizada.

CORTAFUEGOS (firewall)-. Es un ordenador o un programa que conecta una red a Internet, pero impide el acceso no autorizado desde Internet.

Cracker.- Persona que se introduce en computadoras ajenas para causar daño o sacar información con algún beneficio.

CRACKER.- Programa o archivo que permite utilizar, de manera completa, algunas aplicaciones que poseen restricciones para su uso.

Cyber.- Prefijo asociado a palabras relacionadas con Internet, o elementos virtuales.

D

DCD (data carrier detected).- Es el sistema que detecta la portación de datos.

DDE (dynamic data exchange).- Es el Intercambio Dinámico de Datos. Conjunto de especificaciones de Microsoft para el intercambio y el control de flujo entre aplicaciones

DES (data encryption standard).- Es un algoritmo de encriptación de Estándar. Algoritmo desarrollado por IBM, utiliza bloques de datos de 64 bits y una clave de 56 bits. Es utilizado por el gobierno americano.

Dial Up .- Tipo de conexión a un servidor ISP por línea discada o convencional.

DIGITAL CERTIFICATE.- Son documentos digitales emitidos por una empresa (autoridad de certificación), que atestiguan que una clave pública corresponde a un individuo o entidad determinada. Así se evita que intrusos no utilicen esa información.

dns (domain name system).- Systema de nombres de dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. (Ej. www.render.es pasa a 195.76.16.131)

dominio (domain).- Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. (Ej. render.es)

dsp (digital signal procesor).- Es una señal que envía el módem para informar que esta listo.

E

E1.- Es un enlace digital que contiene 30 canales de información, de 64 Kbps, y 2 de sincronización. En total transporta 2.048 Mbps, y es usado en Europa ypaíses de América Latina.

e-mail (electronic mail / CORREO ELECTRONICO).- Sistema de mensajería informática similar al correo tradicional, en varios aspectos y muy distinto en otros. Una de las principales ventajas es la velocidad. Permite enviar y recibir información de forma privada a una o varias personas, desde y hacia cualquier parte del mundo. Cada una de estas personas deberá contar con una dirección de

e-mail con la que se identifica ante los demás usuarios de la red. El servidor o proveedor de internet que cada usuario contrata le brinda un espacio en el disco duro del mismo, para recibir mensajes y luego estos serán enviados a su maquina personal. No es necesario el vinculo directo y simultaneo para recibir los mensajes, de distribuirlos se encarga el servidor.

ENCRIPTar.- Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que solo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito.

Enlace.- Link, vinculo. Es una palabra, frase o gráfico de hipertexto que conecta con otra información. En la www, los enlaces conectan paginas entre si, o sectores dentro de la misma página.

Ethernet.- Popular tecnología de redes de área local (LAN) inventada por Xerox Corporation. Una red Ethernet consiste en un cable al que se conectan las computadoras. Cada uno de ellos, necesita de un hardware conocido como tarjeta de interfaz, para conectar a cada computadora con la red Ethernet. Es un protocolo de enlace de datos

Extranet .- Red que también utiliza el protocolo de comunicación TCP/IP, sin embargo solamente entre redes de empresas diferentes. Es típicamente el modelo de comunicación utilizado entre empresas y sus asociados de negocios.

extension.- Es el sufijo que se utiliza para acompañar a los archivos de manera tal que los clasifiquen por su contenido y tipo de aplicación.

F

Fibra Óptica .- Compuesta básicamente por material dieléctrico (en general sílice), con una larga estructura cilíndrica, transparente y flexible, de dimensiones microscópicas, comparables a las de un cabello humano. Permite altísimas tasas de transmisión, del orden de los 1 Gbps (mil millones de bits por segundo), que dependen, sin embargo, de las limitaciones de los equipos utilizados. Es inmune a interferencias electromagnéticas externas y presenta alto grado de seguridad para la información transportada

fddi (fiber distributed data interface).- Estándar que permite transferir datos a través de fibra óptica a una velocidad de 100 Mbps.

FILE.- Significa archivo o expediente en ingles.

FINGER.- Protocolo de alto nivel que permite obtener información sobre los usuarios que están actualmente conectados a un determinado sistema remoto. Conociendo el nombre de cuenta de un determinado usuario, es posible conocer información detallada acerca del mismo.

FIREWALL.- Literalmente significa "Muro de fuego", es un sistema de seguridad para prevenir a las maquinas de la intromisión de intrusos en sus sistemas operativos. Es similar a "Cortafuegos".

Frame.- Esta palabra significa estructura, cuadro o trama de datos. Esta opción, disponible en los browsers mas recientes, permite dividir la pantalla en varios cuadros independientes. La ventaja es que el usuario nunca perderá de vista el índice de contenido de su site.

FRAME.- Paquete de datos. Cuando la información a enviar es más grande que el cnductor, se la divide en paquetes, y se lo envía de esta manera.

frame relay.- Protocolo de enlace de mediante un circuito virtual permanente muy usado para dar conexión directa a Internet.

FTP (file transfer protocol).- Protocolo de transferencia de ficheros. Una de los mas usados en Internet porque sirve para intercambiar datos de ficheros entre distintas computadoras.

FTP ANÓNIMO.- Es un sistema que permite acceder a un servidor FTP que aporta voluntariamente sus contenidos a la red Internet, pasando estos a ser de acceso publico (no es necesario ningún proceso de identificación para obtenerlos).

G

GATEWAY (PUERTA DE ACCESO).- Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red. En español se conoce también como "pasarela".

gsm (global system mobile comunications).- Sistema global de comunicaciones movibles. Sistema digital de telecomunicaciones principalmente usado para telefonía móvil. Existe compatibilidad entre redes, por tanto un teléfono GSM puede funcionar en todo el mundo.

H

Hacker.- Por este nombre se conoce a los "piratas informáticos". Un pirata informático es aquel capaz de entrar en sistemas cuyo acceso esta restringido. No necesariamente con malas intenciones, pero la mayoría de las veces lo hacen para beneficio propio. Cuando estos entran en un sistema o base de datos con el único fin de hacer daño, se los conoce como "crackers".

hdlc (high-level data link control).- Control de Enlace de Datos de Alto Nivel.

HOST.- Es el nombre genérico dado a una computadora que esta conectada a Internet y cumple la función de Servidor. Permite que su información sea accedida por otras maquinas, a través de un numero IP o un nombre.

I

i pass (roaming).- Con este servicio que brinda el servidor, los usuarios podrán acceder a la red mediante una conexión dial-up en cualquier lugar del mundo, usando una llamada local.

ie (internet explorer).- El *Internet Explorer* es el navegador (software que se utiliza para navegar) fabricado por Microsoft, que viene incluido en el Windows.

Intranet.- Se llama así a las redes que sirven solo para uso interno. Una red corporativa de una empresa que utiliza protocolos TCP/IP y servicios similares como www, puede ser un ejemplo.

ip (internet protocol).- Es el protocolo bajo el que se agrupan todos los demás protocolos de Internet. También esta relacionado con las direcciones de red de Internet.

ip number.- Cada computadora conectada a Internet posee un numero IP. Este numero tiene cuatro partes separadas por puntos. Sirve para identificar a cada maquina en Internet. Alternativamente existen los nombres de dominio que sirven para recordarlos con mas facilidad.

ipx (internet packet exchange).- Intercambio de paquetes entre redes. Inicialmente el protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

ISO. (international standard organization).- Organización Internacional para la normalización. Es una organización de carácter voluntario fundada en 1946 responsable de la creación de normas internacionales en muchas áreas, entre las que se incluyen la informática y las comunicaciones. Esta constituida por las organizaciones de normalización de sus 89 países miembros.

iss (internet security scanner).- Rastreador de Seguridad de Internet. Programa que busca puntos vulnerables de la red con relación a la seguridad.

J

K

Kbps.- Kilobits por segundo. Esta medida proporciona información de la cantidad de miles de bits que pueden ser mandados por segundo, a través de la red. Es la medida que se usa para definir la velocidad de un módem, los mas rápidos son de 56Kbps.

Kilobyte.- Es una medida utilizada para medir cantidades de datos.

L

lan (local area network).- Red de Area Local. Esta diseñada para la conexión de ordenadores en pequeñas distancias. Este tipo de red es de bajo coste y posee una alta fiabilidad, en lo que se refiere a su instalación y funcionamiento.

lapm (link acces procedure for modems).- Procedimiento de Acceso a Enlace para modems.

lcp (link control protocol).- Protocolo de Control de Enlace

linea dedicada.- Línea telefónica alquilada que une permanentemente dos puntos geográficos. Este tipo de líneas son las que permiten una mayor velocidad de transferencia.

Link.- Es un sinónimo de enlace.

Lock.- Quiere decir cerrado o bloqueado en ingles. Generalmente se usa con el fin de avisarle al usuario que una cuenta o acceso a Internet (o también el acceso a un sistema operativo de una maquina) esta protegido por una contraseña.

Login.- Es el identificador de usuario requerido cuando iniciamos una sesión bajo el sistema operativo UNIX. Si este identificador es introducido erroneamente, el servidor del sistema no nos permitirá el acceso a dicha sesión.

LOGIN NAME.- Es el nombre que utiliza cada usuario para denominar su cuenta de acceso al servidor y su dirección de e-mail, y así poder diferenciarla de las otras.

Logon.- Es un sustantivo que significa "ganar acceso" en un sistema informático.

LOGS.- Son informes que realiza cada servidor para su uso interno. Estos informes los realiza el servidor de Internet para conocer en detalle los accesos de cada uno de los usuarios. Los usuarios podrán tener en detalles la cantidad de tiempo que navegaron (por mes) y cuantas veces se conectaron a la red.

M

man (metropolitan area network).- Red de Area Metropolitana.

mb (megabytes).- Es la unidad usada para medir la cantidad de memoria de la computadora o del disco rígido.

Mbone.- Red de Alta Velocidad en EEUU diseñada para la transmisión masiva de imágenes y sonidos en tiempo real.

mnp (microcom networking protocol).- Protocolo de Redes de Microcom. Protocolo de corrección de errores desarrollado por Microcom y muy usado en comunicaciones con módem. Existen varios niveles MNP2 (asíncrono), MNP3 (síncrono) y MNP4 (síncrono).

MLPP (multilink ppp).- Sistema que permite conexión múltiple, mediante dos modems (o pueden ser más) con el servidor. Acelera la transmisión de información.

MODEM 56K.- Dispositivo usado para transferir información en Internet de mayor capacidad en cuanto a la velocidad que los módem standard.

El 56K es una norma que sirve para cualquier marca de módem 56 K. Si estos tipos de módem se conectan a un servidor que tenga habilitado un servicio que maneja esta norma, pueden conectarse a su max. velocidad sin importar la marca del módem que estén usando.

MODEM (modulador / demodulador).- Dispositivo utilizado para la transmisión de información a larga distancia. La vía de transmisión puede consistir en un cable largo o en una conexión telefónica. El módem contiene un modelador (para enviar datos) y un demodulador (para recibirlos).

N

nacr (network announcement request).- Petición de participación en la Red. Es la petición de alta en Internet para una subred o dominio.

nap (network acces point).- Punto de Acceso a la Red. Normalmente se refiere a los tres puntos principales por los que se accede a la red Internet en EEUU.

Ncp (network control protocol).- Protocolo de Control de Red. Es un protocolo del Network Layer.

Net.- Significa red en ingles.

netiquette

Reglas de actuación que suelen respetar los usuarios de la red. Como por ejemplo, no escribir todo con mayúsculas, que equivale a gritar.

Network.- Una o mas computadoras conectadas que interactúan a través de una red.

nic (network information center).- Cualquier organismo que gestione información necesaria para el funcionamiento de una red.

Nic (Network Interface Card).- Tarjeta de red. Conectada a un slot libre de la PC, es la encargada de gestionar las comunicaciones. Es, en definitiva, la que proporciona la conexión física entre la computadora y el cable.

NODO.- Es el punto de unión entre varias redes. Tiene especial importancia, para la rapidez de las conexiones, que la computadora gestora de este punto sea una maquina potente y capaz de soportar un trafico de comunicaciones intenso; puesto que, de lo contrario, se produciría un embotellamiento en el mismo y, como consecuencia, importantes demoras.

NSFNET (national science foundation network).- Red de la Fundación Científica Nacional de EEUU. En sus orígenes era una red de área amplia que conectaba las computadoras de 5 centros de esta fundación utilizando el protocolo TCP/IP y poseía una conexión a Internet. En la actualidad, es una parte esencial de las comunicaciones académicas y de investigación norteamericanas. Es el esqueleto de la red que da cobertura a los EEUU. NSFNET también tiene conexiones fuera de los EEUU, en Canadá, México, Europa y la zona del Pacifico. Esta red es parte de Internet.

NUMERO DIAL-UP.- Es el numero a través del cual una computadora puede conectarse a Internet con el dialer correspondiente. En general estos números son 0610.

O

OSI (open systems interconnection).- Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuestos por la ISO. Divide las tareas de la red en siete niveles.

P

PAP (password authentication protocol).- Protocolo de Autentificación por Password. Permite al sistema verificar la identidad del otro punto de la conexión mediante password.

PAQUETE.- Fragmento de información que se dirige a través de la red a la dirección que le indica su cabecera. Toda la información que se transmite entre computadoras de la red se divide en paquetes de diferentes tamaños, que siguen distintos caminos y que, una vez en su destino, vuelven a agruparse.

PASSWORD.- Clave o contraseña.

PDA (personal digital assistan).- Programa que se encarga de atender a un usuario concreto en tareas como búsquedas de información o selecciones atendiendo a criterios personales del mismo. Suelen tener tecnología de IA (Inteligencia Artificial).

PCI (Peripheral Component Interconnect o Interconexión de Componentes Periféricos) .- Bus local de alto desempeño con un canal de datos entre la CPU y los periféricos de alta velocidad independientes del procesador.

PEER.- En una conexión punto a punto se refiere a cada uno de los extremos.

PEM (private enhanced mail)

PING.- Utilidad que permite averiguar si un determinado sistema remoto esta activo. El mecanismo empleado para esta averiguación consiste en enviar unos paquetes de interrogación especiales (usando el protocolo de control ICMP) a la maquina especificada (con un nombre o una dirección IP), y la tarjeta de red se encargara de devolver un eco de los mismos a su origen señalado que el sistema esta activo.

plug-in.- Son programas que permiten visualizar e interpretar ficheros de texto de video o de sonido de distinto formato. Con ellos se puede visualizar tanto animaciones o gráficos, como introducirse en mundos tridimensionales e incluso sintonizar aplicaciones de radio emitidos por internet. La característica fundamental de los plugs-in es que no son transparentes para el usuario que los usa y están integrados en los browsers. Para instalarlos solo será necesario importar el fichero comprimido, que puede conseguirse de forma gratuita en la red y ejecutar su rutina de instalación en la computadora del usuario.

PORT.- Es el lugar de donde sale o entra información de una computadora. Los modems están conectados a un puerto especial. Hay otros puertos que se utilizan para accesorios periféricos como impresoras o scanners.

ppp (point to point protocol).- Protocolo punto a punto. Protocolo de Internet para establecer enlace entre dos puntos. Es un protocolo que se utiliza para el envío de paquetes de TCP/IP por la línea serie del ordenador. (Pej entre el usuario y el servidor)

PROTOCOL (PROTOCOL).- Son las normas que deben cumplir dos o mas computadoras para intercambiar mensajes entre si. El protocolo describe tanto el formato de los mensajes como la forma de respuesta a cada uno de ellos.

PROXY SERVER.- La empresa se diferencia de sus competidores por el uso efectivo de la tecnología Proxy, que beneficia al usuario en dos aspectos importantes. Por un lado, la velocidad con referencia a la conexión y la búsqueda de información en la red; y por otro, la seguridad que necesitan los usuarios en el momento de preservar la identidad de información que envían o reciben, o la posible infección de la información con virus que circulan por la web. Este tipo de tecnología es muy eficiente si se puede lograr utilizarlo en forma adecuada, de lo contrario puede llegar a ser ineficaz.

PUERTO.- Toda conversación TCP/IP entre una aplicación servidora se realiza empleando un numero común denominado puerto, de modo parecido a los canales que emplean las emisoras de radio. La mayoría de los protocolos de alto nivel de Internet

poseen un puerto standard, aunque pueden emplear otros números como puertos alternativos.

Q

R

RDSI (red digital de servicios integrados).- Red telefónica con anchos de banda desde 64Kbps. Similar a la red telefónica de voz en cuanto a necesidades de instalación de cara al abonado, pero digital. En Ingles ISDN.

RED.- Grupo de computadoras y dispositivos conectados unos con otros para comunicarse y transmitir datos entre ellos.

RECURSOS.- Son los dispositivos que se comparten en la Red, como: los discos rígidos, lectoras de CD, impresoras, escaners, entre otras cosas.

Router.- Es una computadora con fines especiales. Se dedica exclusivamente a la conexión entre dos redes y a encaminar los paquetes de información de una a otra. Es un ordenador que se encarga de transmitir datos desde su nodo a otro nodo para que la información llegue a su destino (un eslabón de la cadena de transmisión)

RSA (rivest, shamir, adelman).- Public Key Encryption Algorithm. Algoritmo de encriptación de clave publica desarrollado por Rivest, Shamir y Adelman.

RTP (real time protocol).- Protocolo de tiempo real. Protocolo utilizado para la transmisión de información en tiempo real, como es el audio y el video en una videoconferencia.

RWIN (receive window).- Ventana de recepción. Parámetro de TCP que determina la cantidad máxima de datos que puede recibir la computadora que actúa de receptora.

S

SDH (Synchronous Digital Hierarchy) - Arquitectura de multiplexación y de transmisión de señales digitales entre elementos de redes cuyas señales de reloj de muestreo son sincronizadas con exactitud. La velocidad de transmisión es de 155 Mbps.

SDLC (syncronous data link controller).- Controlador de enlaces de Datos Sincrónico. Se trata de un protocolo para enlace sincrónico a través de líneas telefónicas.

SERVERS / SERVIDORES.- Computadora principal de un sistema que se encarga de distribuir los programas y modos operacionales a sus usuarios. Según el software de red que se utilice, se cumplirán requisitos en cuanto al procesador y la memoria de cada maquina. Cuanto más rápido sea el servidor, mejor funcionara la red, porque ganara en eficiencia.

SERVICIO 0610.- Servicio que brindan las compañías telefónicas para tener conectividad a Internet, a un precio reducido (hasta un 50% de descuento). El servicio

sirve para conectar la computadora del usuario con el servidor mediante un acceso Dial-up.

SLIP (SERIAL LINE INTERNET PROTOCOL).- Línea de serie IP. Antiguo protocolo de transmisión de información de internet por vía telefónica que ha sido casi totalmente sustituido por el llamado PPP, de la familia TCP/IP.

SNIFFER.- Literalmente "Husmeador". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal.

snmp (simple network mangment protocol).- Protocolo para gestionar grandes redes.

Sprinet. Red de comunicaciones avanzadas instalada en el entorno de la UPV/EHU y extendida a Centros de I+D (Investigación + Desarrollo). Nació tras el acuerdo de colaboración entre la Sociedad para la promoción y Reconversión Industrial (SPRI) y la UPV/EHU. Fue diseñada desde el principio para contemplar la implantación de servicios de comunicaciones de voz, datos e imagen.

SSL (Secure Sockets Layer).- Protocolo de Internet desarrollado para transferencia y acceso de datos con seguridad a partir de browsers. Es muy utilizado para transacciones comerciales vía Internet.

STM-1. - Estándar que representa 155 Mbps (Megabits) por segundo en la transferencia de datos.

Switch.- Equipo utilizado para conectar segmentos de redes locales, análogo a un puente con múltiples puertos, sin embargo, al contrario de los puentes que usan bus interno compartido, los switches permiten que las estaciones transmitan simultáneamente
en segmentos separados .

T

T-1. -Es un tipo de conexión que permite transferencias de hasta 1.5MB/segundo.

T-3.- Otro tipo de conexión que permite transferir datos hasta 45Mb/segundo. Generalmente estas conexiones de alta velocidad se utilizan para transferir grandes volúmenes de datos.

tcp (transmission control protocol).- Protocolo de control de transmisión. Uno de los protocolos de transmisión mas usados en Internet. Es un protocolo del Transporter Layer.

Se encarga de dividir la información en paquetes cuando la información de origen todavía no fue enviada, para luego recomponerla en el lugar de destino.

TCP/IP (TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL).- Traducido literalmente, son los nombres de los protocolos que especifican como se comunican los ordenadores en Internet. Surgieron en 1974 a raíz de investigaciones

para el intercambio de paquetes de información dentro de la red ARPANET. Los servicios básicos que proporciona son tres: transferencia de ficheros, identificadores de usuarios a huéspedes remotos y correo electrónico. Para que dos o mas computadoras se comuniquen a través de Internet, deben poseer software TCP/IP.

telnet.- Tele Red. Conexión a un host en la que el ordenador cliente emula un terminal de manera que se configura como terminal virtual de la computadora que funciona como servidor. Mediante esta aplicación es posible conectarse a una maquina remota

TX .- Abreviatura de transmisión.

U

unix .- Sistema operativo de tiempo compartido (la computadora puede ser utilizada por varios usuarios a la vez) desarrollados por los laboratorios norteamericanos AT&T Bell.

UPLOAD.- Es la transferencia de datos de una computadora a otra (generalmente del cliente al servidor) a través de Internet.

UPS/Geradores/PDU – (Uninterrupted Power Supply) .- En caso de falta de energía, la UPS proporciona inmediatamente energía de reserva. Después de haber sido encendidos y "calentados", los generadores se adelantan y pasan a suministrar la energía a los equipos. Durante el proceso de recuperación de energía, los PDUs nivelan el suministro de energía evitando picos y caídas bruscas.

USER (USUARIO).- Es el cliente que usa los servicios de Internet.

USERNAME (NOMBRE DE USUARIO).- Es un sinónimo de login name. Es usado por el usuario para diferenciar su cuenta de todas las otras en la red.

UUCP (unix to unix copy program).- Protocolo de AT&T para la transferencia de archivos entre maquinas UNIX (con versiones para otros sistemas operativos). Muy empleado para la difusión de las News de Usenet y de Correo Electrónico, tiende a desaparecer con la progresiva expansión de Internet.

USB (Universal Serial Bus) .- Estándar "plug-and-play" para conectar varios dispositivos de entrada/salida a un único puerto de gran ancho de banda.

V

VPN (Virtual Private Network).- Grantiza el uso seguro de una red pública, tal como Internet. A través de VPN, los accesos a los datos entre redes de la empresa y entre usuarios y la empresa son codificados, ofreciendo total seguridad a los usuarios y a la red de acceso.

W

WAN (wide area work).- Red de área extensa. Está diseñada para abarcar grandes distancias geográficas. Dispone de una pequeña computadora de uso exclusivo en cada nodo, que se conecta a la línea de transmisión y mantiene operando la red, independientemente de las computadoras que la utilicen. La computadora de uso exclusivo recibe el mensaje proveniente de otro lugar y lo entrega a una de las computadoras locales. Acepta mensajes de cualquier PC local y los envía a través de una línea de transmisión a su destino.

WAP (Wireless Access Protocol).- Es una especificación abierta y global que permite al usuario de dispositivos wireless, tales como celulares, pagers o palm tops, tener acceso fácil e interaccionar instantáneamente con informaciones y servicios.

WEB.- Es sinónimo de Internet o world wide web.

Windows.- Pseudo sistema operativo. Se trata de un entorno gráfico con algunas capacidades multitarea. La versión actual WINDOWS 98 funciona parcialmente a 32 bits.

WINSOCK .- Programa standard creado por Microsoft usado para la conexión a Internet y a otras redes.

WebTrends - Producto utilizado por proveedores y empresas que permite el análisis de estadísticas de acceso a los servidores Web.

Wireless (Inalámbrico) - Tecnologías que utilizan el aire como medio de transmisión (satélite, microondas y spread spectrum).

X

Y

Z

Bibliografia

1.-Alarcon, Jose M. (2004). Seguridad para redes inalámbricas. URL; http:// www.krasis.com

2.-Aguirre, José E. (2000). Redes Inalámbricas. URL; http://wwww.lafacu.com/apuntes/informatica/redes_inalamb/default.htm

3.- Bazaraa, Mokhter S., Programación lineal y flujo en redes, Limusa, 1981

4.- Black Uyless. Redes de computadores, protocolos, normas e interfaces, segunda edición, Colombia, Alfaomega.

5.- Buet Santana, Vicente (1998). Redes inalámbricas de área local. URL; http://wwwtimagazine.net/magazine/0798/wireles.cfm

6.- Caballero M. Jose. Redes de banda ancha, primera edición, Mexico, Alfaomega, 1999

7.- Caballer Xavier. (2004). Redes inalámbricas. URL; http:// http://www.aftenposten.no/english/local/article.jhtml?articleID=431326

8.- Caballer Xavier. (2004). Redes inalámbricas. URL; http:// http://www.hispasec.com/unaaldia.asp?id=1243

9.- García Tomás Jesús, Ferrando Santiago, Piattini Mario. Redes de alta velocidad, primera impresión, España, Enero 1997.

10.- Gonzalez Sainz, Nester, Comunicaciones y redes de procedimientos de datos, Bogota, Mc Graw Hill, Mexico 1987.

11.- Grupo Penteo (2001) ¿Qué son las redes inalámbricas?, URL; http://www.expansionyempleo.com/edicion/noticia/0,2458,41089,00.html

12.- Introducción a la redes inalámbricas por Microsoft, http://www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp

13.- Jenkins Neil, Schatt Stan. Redes de area local (LAN) Introducción facil a los conceptos y los productos de redes, México 1996. Editorial Sems Publishing.

14.- Ley Federal de Telecomunicaciones, disposiciones generales 2005.

15.- Martinez Mendes Francisco J. (2003) Telemática y teledocumentación: modelos de referencia. URL; http://um.es/~gtiweb/fjmm/ttsiteplan2/modelos.htm#inicio

16.- Menasce Daniel A., Redes de computadoras aspectos técnicos y operacionales, paraninfo Madrid 1988

17.- Merike Kaeo , Diseño de seguridad en redes, traducción Santiago Fraguas Beraooin, Pearson educación Madrid 2003, pág. 146

18.- Metarie C., Polian Nicole. Teoria y programación de las redes, 1989 Madrid.

19.- Morguet Carlos V.(2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php

20.- Palazón, Francisco J. (2002), Nuevas tecnologías: adios al cable, URL; http://www.telyco

21.- Pierre Armond. Redes locales e internet introducción a la comunicación de datos, editorial Trillas.

22.- Rabago, Jose Felix, Redes locales: conceptos basicos, Madrid, 1989

23.- Raya, Jose Luis, Redes locales y TCP/IP, Computec, 1997

24.- Raya Cabrera, Jose Luis, Alta velocidad y calidad de servicio en redes IP, Alfaomega, 2002

25.- Schatt, Stanley. Redes locales: conceptos básicos, Anaya multimedia, 1989.

26.- Una experiencia de instalación de una red inalámbrica
http://www.arturosoria.com/eprofecias/art/wireless.asp

27.- Red Inalámbrica Pública en México

http://www.miembrosprodigy.com.mx/prodigymovil

Referencias

1) Ley Federal de Telecomunicaciones, disposiciones generales, cap. 1 art. 3, fracción I ,II, VII, IX, X, XI,. XII, XIV.

2) Ley Federal de Telecomunicaciones, disposiciones generales, cap. III, IV,V ,.

3) García Tomás Jesús, Ferrando]Santiago, Piattini Mario. Redes de alta velocidad, primera impresión, España, Enero 1997, pag. 101.

4) Black Uyless. Redes de computadores, protocolos, normas e interfaces, segunda edición, Colombia, Alfaomega, 1997, pag. 7, 33, 77, 79, 162-168, 495, 225, 556, 557

5) Redes de computadores, protocolos, normas e interfaces, segunda edición, Colombia, Alfaomega, 1997, pag. 172

6) García Tomás Jesús, Fernando Santiago, Piattini Mario. Redes de alta velocidad, primera impresión, España, Enero 1997, pag. 152.

7) Merike Kaeo , Diseño de seguridad en redes, traducción Santiago Fraguas Beraooin, Pearson educación Madrid 2003, pág. 146

8) Caballero M. Jose. Redes de banda ancha, primera edición, Mexico, Alfaomega, 1999, pag. 37,189.

9) Buet Santana, Vicente (1998). Redes inalámbricas de área local. URL; http://wwwtimagazine.net/magazine/0798/wireles.cfm

10) Aguirre José E. (2000).Redes Inalámbricas. URL; http://wwww.lafacu.com/apuntes/informatica/redes_inalamb/default.htm

11) Grupo Penteo (2001) ¿Qué son las redes inalámbricas?, URL; http://www.expansionyempleo.com/edicion/noticia/0,2458,41089,00.html

12) Martinez Mendez Francisco J. (2003) Telemática y teledocumentación: modelos de referencia. URL; http://um.es/~gtiweb/fjmm/ttsiteplan2/modelos.htm#inicio

13) Palazón, Francisco J. (2002), Nuevas tecnologías: adios al cable, URL; http://www.telyco

14) Morguet Carlos V. (2003). Seguridad para redes. URL;http://www.seguridadenlared.org/es/wireles.php
15) Alarcon Jose M., (2004). Seguridad para redes inalámbricas. URL; http:// www.krasis.com
16) Caballer, Xavier. (2004). Redes inalámbricas. URL; http:// http://www.hispasec.com/unaaldia.asp?id=1243