UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

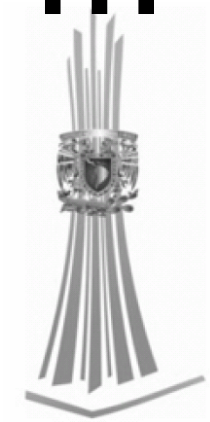
FACULTAD DE ESTUDIOS SUPERIORES ARAGON

"ESTRATEGIA DE DISEÑO DE REDES INALÁMBRICAS DE USO PERSONAL PARA MULTIACCESO A INTERNET"

T E S I S

QUE PARA OBTENER EL TITULO DE INGENIERO MECANICO ELECTRICISTA PRESENTAN:

MYRNA LEON CORTES
HIPÓLITO ISRAEL RAMÍREZ CISNEROS



ASESOR: ING. ENRIQUE GARCIA GUZMAN

MEXICO , 2007

INDICE

CAPÍTULO 2: REDES COMUNES

CAPÍTULO 3: REDES INALÁMBRICAS

INTRODUCCIÓN

INTRODUCCIÓN

Desde sus inicios, el hombre ha buscado incansablemente medios para comunicarse eficientemente. Esta búsqueda ha permitido el desarrollo del hombre que, visto desde el nivel físico de su evolución y hasta llegar a la era moderna, se ha visto apoyado por herramientas que extendieron su funcionalidad y poder como ser viviente.

Siendo conciente de la habilidad creativa que poseía, el hombre fue elaborando métodos y procedimientos para organizar y preservar el conocimiento que tenía y de incrementarlos, así como los recursos con los que contaba, manipulando, a su vez su entorno; siempre buscando su propio beneficio, impulsando la ciencia y mejorando su nivel de vida. Esto, aún a costa de sacrificar el desarrollo natural de su ambiente, produciendo así todos los adelantos que un gran sector de la población conoce como: automóviles, aeroplanos, trasatlánticos, teléfonos, televisores, etcétera.

A la par de este desarrollo, evolucionó dentro del sector tecnológico el cómputo electrónico. Este nació con los primeros ordenadores en la década de los años 40, ya que la necesidad del momento era extender la rapidez del cerebro humano para realizar algunos cálculos aritméticos y procedimientos repetitivos.

Para continuar avanzando, este esfuerzo se fijó en crear unidades de procesamiento cada vez más veloces, divididas en cuatro generaciones bien definidas:

- La primera con tubos al vacío,
- La segunda con transistores,
- La tercera con circuitos integrados y
- La cuarta con circuitos integrados que permitieron el uso de computadoras personales y el desarrollo de las redes de datos.

Este último punto es de vital importancia, puesto que nos habla de un avance enorme en el cual ya existe la comunicación “directa” a larga distancia y a una gran velocidad, como si tuviéramos enfrente a aquel con el que compartimos información. Y de eso se trata, las redes de ordenadores, basan su funcionamiento en "compartir recursos", y uno de sus objetivos principales es hacer que todos los programas, datos y hasta los propios equipos estén disponibles para cualquier usuario que así lo solicite, sin importar la localización física del recurso y del propio usuario.

Inicialmente, las redes tenían muchos problemas debido a su complejidad; detalles que se han ido depurando con el paso del tiempo.

Actualmente, las redes son muy útiles para el hombre, éstas pueden ser inalámbricas, que es de lo que se trata el presente trabajo.

Las redes inalámbricas tienen dos utilidades principales: en el manejo de la información como tal y en la comunicación móvil.

Se pretende abarcar los aspectos elementales de esta tecnología en este proyecto y darlo a conocer de la forma más clara posible.

Se sabe que la búsqueda de conocimiento nunca llegará a su fin.

Cabe mencionar que una de las tecnologías más interesantes en la actualidad son las redes de área local inalámbricas.

Esta tecnología ha permanecido en un estado de receso en los últimos años; sin embargo, genera ganancias millonarias alrededor del mundo.

El estándar predominante de esta tecnología es recopilado por el IEEE, que cuenta con una gran variedad de grupos de trabajo realizando tareas alrededor de 802.11.

En la actualidad, esta materia y su entendimiento, son aspectos muy importantes, de la misma manera que el enfoque a la seguridad y a la movilidad en general.

La conexión de computadoras mediante ondas de radio o luz infrarroja (redes inalámbricas), es tema de muchas investigaciones actuales.

Una de las principales ventajas de las redes inalámbricas es que facilitan la operación en donde la computadora no puede permanecer en un solo lugar, como el caso de almacenes o de oficinas.

No se espera que las redes inalámbricas lleguen a desplazar a las redes cableadas, puesto que éstas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. (2Mbps vs. 10 Mbps).

A pesar de esta gran desventaja, se espera que, en un futuro no muy lejano, se pueda realizar una red híbrida, que absorba los beneficios de una red inalámbrica y de una red cableada, ampliándose la gama de posibilidades de uso.

CAPÍTULO 1:

INTRODUCCIÓN A REDES DE INFORMÁTICA

CAPITULO 1

INTRODUCCIÓN A REDES DE INFORMÁTICA

Una red se define como un sistema en donde los elementos que lo componen son autónomos y están conectados entre sí por medios físicos y/o lógicos; y que pueden comunicarse para compartir recursos.

1.1 Composición de una red

En su forma más simple, una red puede definirse como el intercambio de información entre dos estaciones de trabajo a través del mismo medio.

Bajo esta visión, los elementos básicos serían:

- Fuente
- Transmisor
- Vía o medio de transmisión
- Receptor
- Destino

Esquemáticamente, esto podría observarse en la figura 1.1

Figura 1.1 Diagrama de bloques de una red informática

En donde:

- La fuente es el dispositivo que genera los datos que serán transmitidos; éste puede ser una terminal o un servidor.
- Los transmisores emiten señales generadas por las fuentes; en ocasiones se requiere de convertidores analógico/digital o digital/analógico para modularlas
- El sistema de transmisión es la vía o canal por donde viaja la información.

- El receptor es un controlador que recibe las señales analógicas y las convierte en digitales.
- El destino sólo recibe información proveniente de la fuente.

El elemento que se encarga de convertir (modular) las señales, es el módem. Esta estructura se puede observar en la figura 1.2:

Figura 1.2 Estructura básica de una red de comunicaciones

Manejando otra visión, podemos decir que, una red informática está formada por un conjunto de ordenadores intercomunicados entre sí que utilizan distintas tecnologías de hardware/software. Las tecnologías que utilizan (tipos de cables, de tarjetas, dispositivos...) y los programas (protocolos) varían según la dimensión y función de la propia red.

Independientemente a esto, definir el concepto de red implica diferenciar entre el concepto de red física y red de comunicación.

Con respecto a la estructura física, los modos de conexión física, los flujos de datos, etcétera; una red la constituyen ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento...) o software (aplicaciones, archivos, datos, información...).

Desde una perspectiva más comunicativa, podemos decir que existe una red cuando se encuentran involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios).

En fin, una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

En su forma más simple una red puede estar constituida por tal sólo dos ordenadores.

Normalmente, cuando los ordenadores están en red pueden utilizar los recursos que los demás pongan a su disposición en la red (impresoras, módem), o bien acceder a carpetas compartidas. El propietario (técnicamente llamado administrador) de un ordenador en red puede decidir qué recursos son accesibles en la red y quién puede utilizarlos.

1.2 Lenguajes de red

Para poder comunicarse entre sí, los ordenadores o las partes de una red deben hablar el mismo lenguaje.

Los lenguajes de comunicaciones reciben el nombre técnico de "protocolos"**,** y en una misma red pueden convivir distintos tipos de protocolos.

Independientemente de los protocolos, es importante que en una red se tenga acceso a información en la lengua natural de las personas; esto es, si la información en la red está en inglés, por ejemplo y una parte de los usuarios no conoce este idioma, la red pierde eficiencia.

1.3 Tipos de redes

Las redes pueden ser catalogadas de diferentes formas, las más utilizadas son: con respecto a su uso; en base a su propiedad; con respecto al tipo de cobertura.

1.3.1 Clasificación según la utilización por parte de los usuarios

- Redes Compartidas. Son aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transmisiones de otra naturaleza.

- Redes exclusivas. Aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

1.3.2 Clasificación con respecto a la propiedad a la que pertenecen dichas estructuras

- Redes privadas, aquellas que son gestionadas por personas particulares, empresa u organizaciones de índole privado, en este tipo de red solo tienen acceso los terminales de los propietarios.

- Redes públicas, aquellas que pertenecen a organismos estatales y se encuentran abiertas a cualquier usuario que lo solicite mediante el correspondiente contrato.

1.3.3 Clasificación según la cobertura del servicio

- LAN (Local Area Network). Creada en el seno de una oficina, nace por necesidad y puede enlazar de dos ordenadores en adelante
- MAN (Metropolitan Area Network).
- WAN (Wide Area Network). Conecta ordenadores que distan mucho entre sí, como los que puede haber entre distintas sedes de una multinacional.
- Internet: una especie de red meta formada por otras 250.000 subredes y por decenas de millones de usuarios
- Intranet: son redes de empresa a las que, por motivos de seguridad, no pueden acceder todos los usuarios de Internet.
- Extranet: conectan las redes de distintas empresas y, muy a menudo, estas tampoco son accesibles
- Ethernet. Es la tecnología más utilizada para interconectar ordenadores en la red. A menudo vienen incluidas en la placa base de los nuevos ordenadores y con ellas se pueden utilizar más protocolos de comunicación, incluso simultáneamente.
- Redes inalámbricas.

1.4 Objetivos de una red

Los objetivos fundamentales de una red son:

- Utilizar los recursos que los demás pongan a su disposición en la red.
- Acceder a carpetas compartidas.
- Reducir la duplicidad de trabajos.
- Uso de correo electrónico para enviar o recibir información.
- Establecer enlaces con computadoras de gran potencia que hagan las veces de servidor, permitiendo y propiciando que los recursos disponibles sean accesibles para todos los ordenadores conectados.
- Mejoramiento de la seguridad y control de la información.

1.5 Topologías de red

Se denomina topología a la forma geométrica en que están distribuidas las terminales, nodos y enlaces que conforman una red.

1.5.1 Objetivos de una topología

El objetivo fundamental de la topología es buscar la forma más económica y eficaz de conectar los diferentes elementos de una red para:

- Facilitar la fiabilidad del sistema,
- Evitar los tiempos de espera en la transmisión de datos,
- Permitir un mejor control de la red y
- Permitir, de forma eficiente, el aumento de las estaciones de trabajo

1.5.2 Consideraciones para la elección de topologías

Se pueden observar dos aspectos al momento de considerar una topología:

- La topología física, que es la disposición real de las máquinas, dispositivos y cableado en la red.

- La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes son: broadcast (Ethernet), y transmisión de tokens (Token ring).

1.5.3 Tipos de topologías usuales

Por sus características, las topologías son usadas en mayor o menor medida, siempre buscando la plena satisfacción del usuario.

Recordemos que la finalidad de una red informática es la de satisfacer los requerimientos de manejo y control de información por parte del usuario, de la mejor manera posible.

Las topologías más utilizadas son:

- Topología de bus
- Topología de estrella
- Topología de anillo

1.5.3.1 Configuración en bus

En este tipo de configuración, las terminales están conectadas a un único canal de comunicación.

Esta topología permite que todas las terminales reciban la información que se transmite; una terminal se encarga de transmitir y las terminales restantes reciben (escuchan) la información.

Básicamente, consiste en un cable con un controlador en cada extremo, del que se cuelgan todos los elementos de una red; esto es, todos los nodos de que consta la red están conectados a este cable, el cual recibe el nombre de “Backbone Cable”.

Tanto Ethernet como Local Talk pueden utilizar esta topología.

El bus es pasivo, esto es, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

La forma de representar una configuración de bus se observa en la figura 1.3

Figura 1.3 Topología de bus

1.5.3.2 Configuración en estrella

En esta topología, las estaciones están conectadas directamente al servidor y todas las comunicaciones se han de hacer necesariamente a través de él.

Esto es, los datos fluyen desde el emisor y hasta el controlador, el cual realiza todas las funciones de la red, además de tomar la función de amplificador.

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

La representación de esta topología se observa en la figura 1.4:

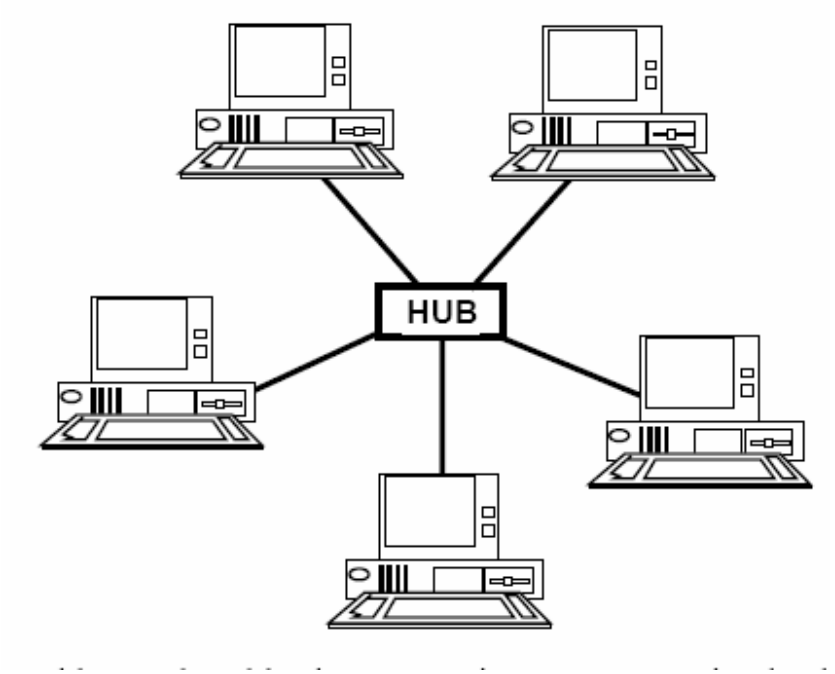


Figura 1.4 Topología en estrella

1.5.3.2.1 Configuración en estrella extendida

La configuración en estrella extendida es una variante de la topología de estrella, y también es llamada topología de malla o trama.

En esta topología se busca tener una conexión física entre todos los ordenadores de la red, utilizando conexiones punto a punto, lo que permitirá que cualquier ordenador se comunique con otros de forma paralela si fuera necesario.

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

La esquematización de esta topología se observa en la figura 1.5:

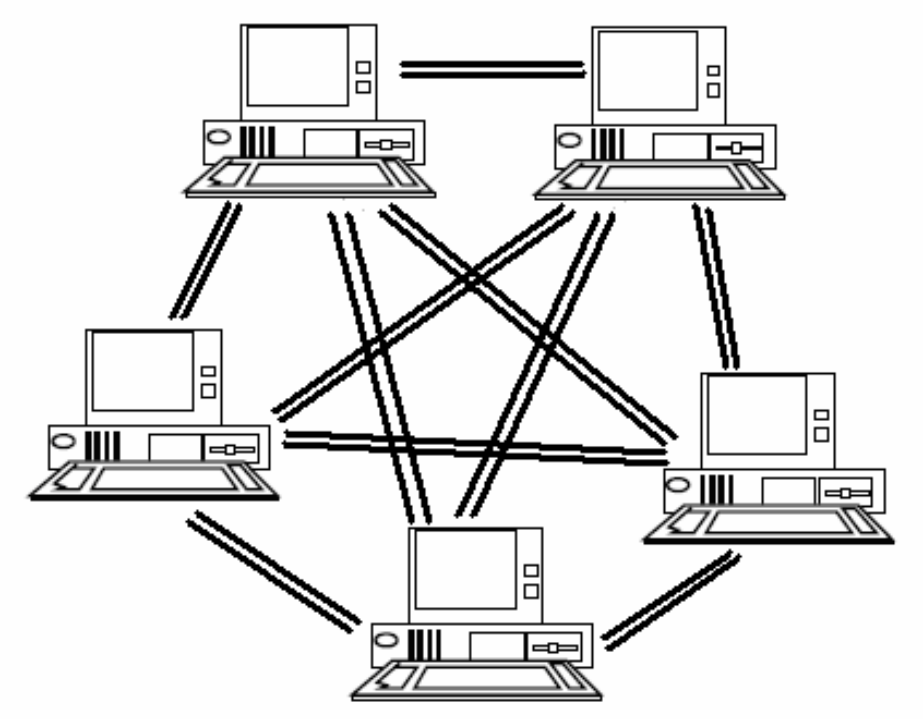


Figura 1.5 Configuración de estrella extendida

1.5.3.2.2 Configuración en árbol

En esta topología los nodos están conectados en forma de árbol. Desde una visión topológica, esta conexión es semejante a una serie de redes interconectadas.

Como la topología de estrella extendida, la configuración en árbol es una variante de la topología de estrella.

Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

Su esquematización se marca en la figura 1.6:

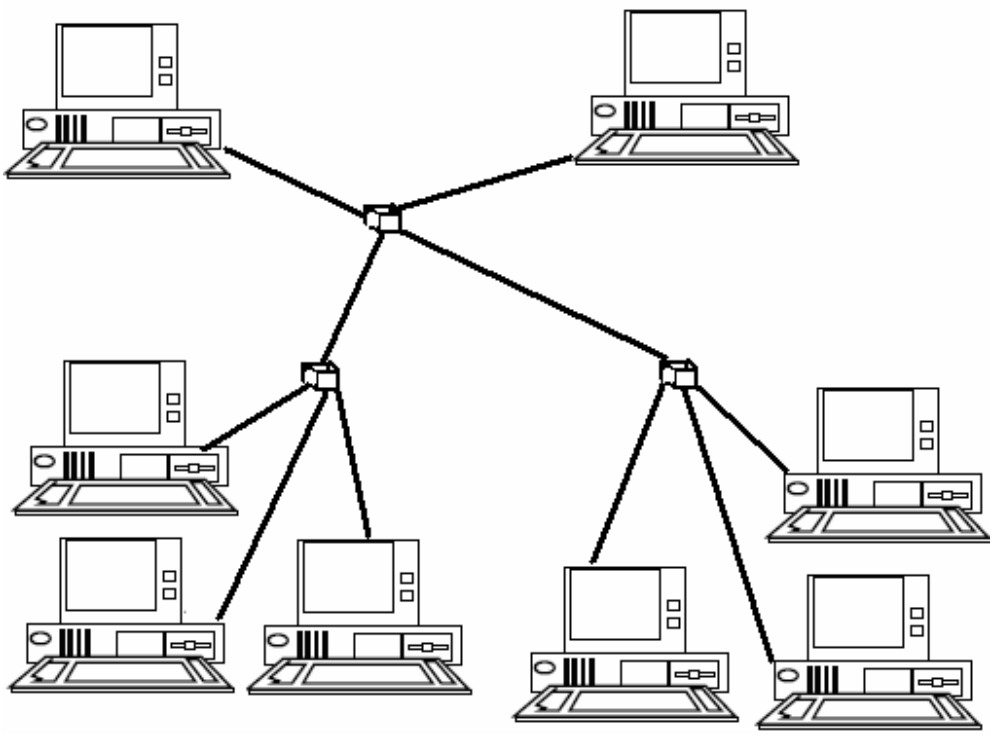


Figura 1.6 Configuración de árbol

1.5.3.3 Configuración en anillo

En esta topología, las terminales se conectan formando un anillo. Es decir, cada una está conectada a la siguiente y la última está conectada a la primera

Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo.

La desventaja de la configuración de anillo, es que si se rompe una conexión, se cae la red completa.

Su esquema se muestra en la figura 1.7

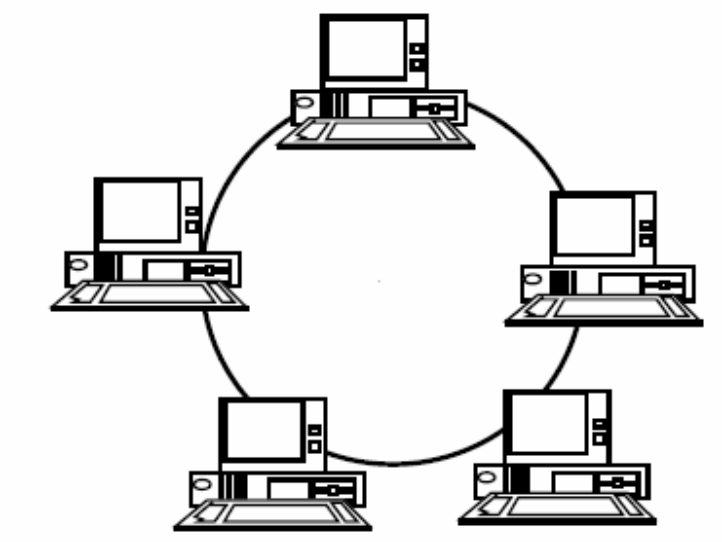


Figura 1.7 Topología de anillo

1.5.4 Topologías híbridas

De acuerdo con las necesidades de los usuarios, las topologías más usuales, vistas anteriormente, se pueden combinar para formar una configuración mixta.

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

La finalidad de crear estas complejas topologías es incrementar la eficiencia y confiabilidad de la red en uso.

Estas combinaciones, se pueden observar en la figura 1.8:

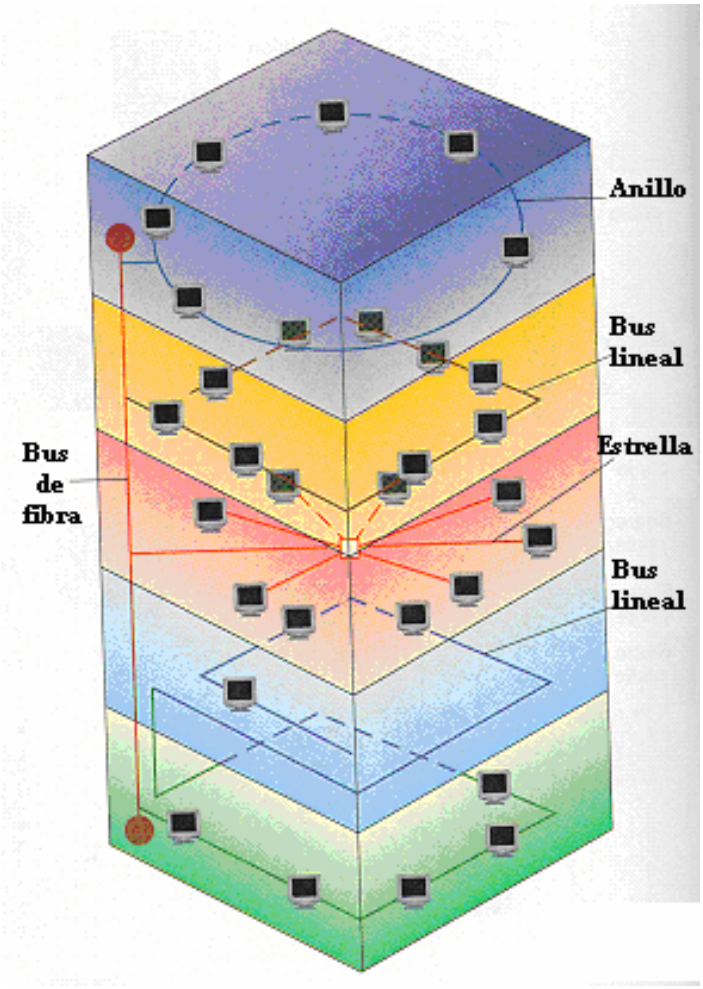


Figura 1.8 Topologías híbridas

1.5.4.1 Anillo en estrella

Esta configuración se utiliza con la finalidad de facilitar la administración de la red.

Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo. Esto se observa en la figura 1.9:

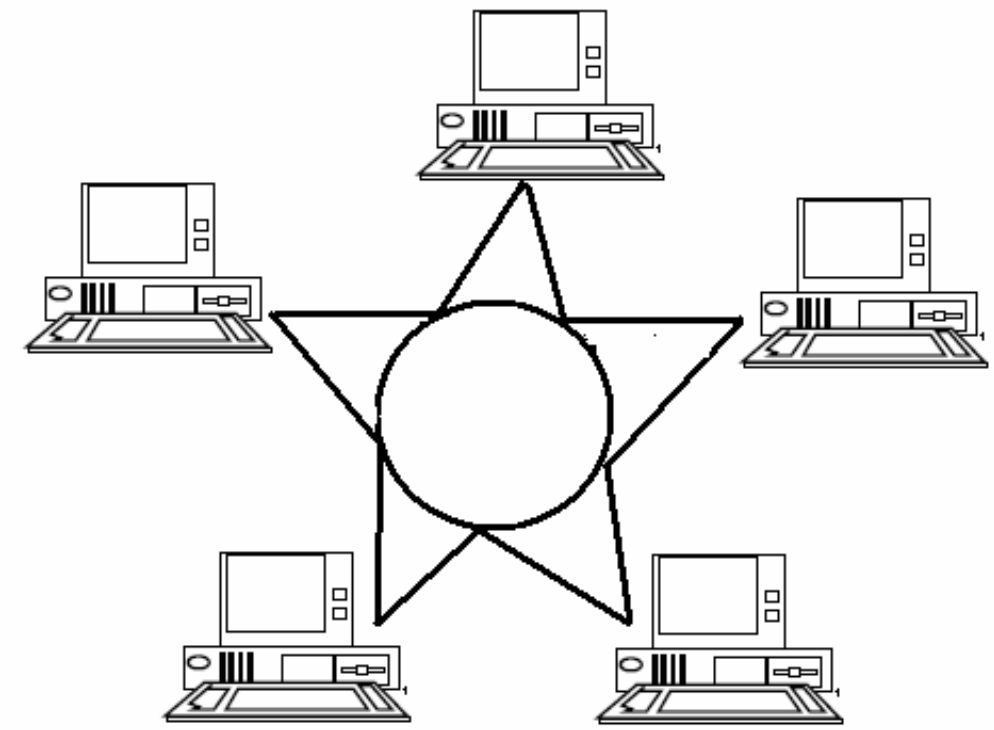


Figura 1.9 Configuración de anillo en estrella

1.5.4.2 Bus en estrella

Como en la topología de anillo en estrella, la finalidad de ésta configuración es facilitar la administración de la red

En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Esquemáticamente se podría observar como en la figura 1.10:

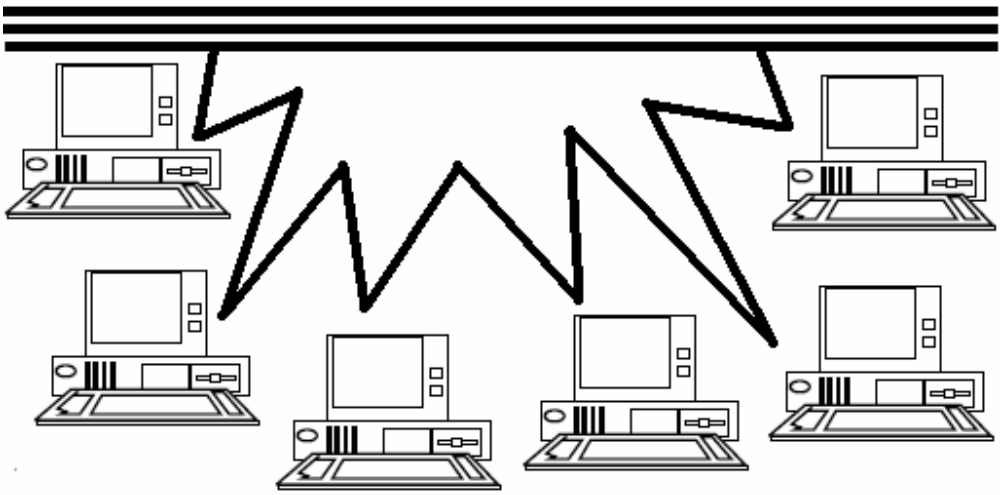


Figura 1.10 Configuración de bus en estrella

1.5.4.3 Estrella jerárquica

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formas una red jerárquica.

Se puede observar su configuración en la figura 1.11:

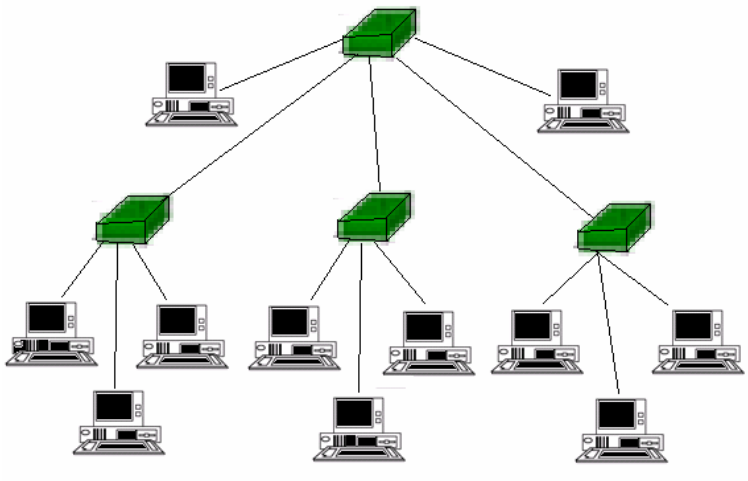


Figura 1.11 Configuración de estrella jerárquica

1.6 Métodos de transmisión

Los métodos de transmisión de datos se relacionan con la capacidad del medio para transmitir información. El ancho de banda indica la capacidad del medio.

Se puede definir al ancho de banda como la diferencia entre la frecuencia más alta y la más baja de una determinada onda. El término, en sí, hace referencia a la capacidad del medio de transmisión; esto marca que, cuanto mayor sea el ancho de banda, la transferencia de datos será más rápida.

Por encima del ancho de banda, las señales tienden a crear perturbaciones en el medio, las cuales interfieren con las señales sucesivas. En función de la capacidad del medio, se hable de transmisión en banda base o transmisión en banda ancha.

Para observar gráficamente el comportamiento de los medios de transmisión, veamos la figura 1.12

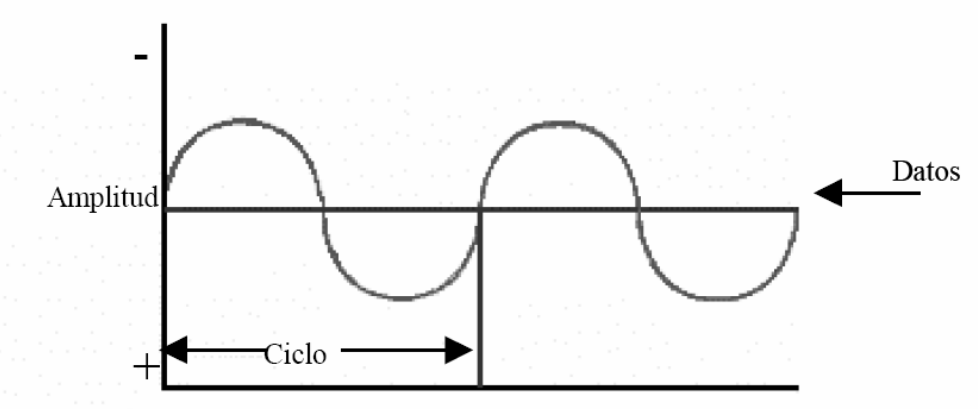


Figura 1.12 Transmisión de datos

Las redes en banda base trabajan, generalmente, con mayor velocidad de transmisión que las de banda ancha, aunque la capacidad de transmisión de éstas, por varios canales simultáneamente, pueden hacer que el flujho total de datos sea básicamente el mismo en ambos sistemas.

1.6.1 Banda base

En el ámbito de las telecomunicaciones, el término de banda base se refiere a la banda de frecuencias producida por un transductor (como un micrófono, un manipulador telegráfico o algún otro dispositivo generador de señales) antes de sufrir una modulación.

Es decir, la banda base es la señal de una sola transmisión en un solo canal; significa que lleva más de una señal y cada una de ellas es transmitida en diferentes canales, hasta su número máximo de canal.

Su uso, en los sistemas de transmisión, se basa en modular una portadora. Durante el proceso de demodulación, se reconstruye la señal banda base original. Bajo esta visión, se puede decir que describe el estado de la señal antes de la modulación y la multiplexación; así como después de la demodulación y la demultiplexación.

Las frecuencias de banda base son, generalmente, mucho más bajas que las resultantes, cuando éstas se usan para modular una portadora o subportadora. Podría decirse que la banda base es la frecuencia de una señal igual, en ancho de banda, a la comprendida entre la frecuencia cero y la frecuencia máxima de codificación.

1.6.2 Banda ancha

La banda ancha se refiere a la transmisión de datos en donde se envían simultáneamente varias piezas de información, con el objetivo de incrementar la velocidad de transmisión efectiva. También es entendida como un método en el cual dos o más señales comparten un mismo medio de transmisión.

1.7 Medios de comunicación en redes

Un medio de transmisión puede definirse como el soporte físicos utilizado para el envío de datos a través de la red.

La mayoría de las redes actuales, utilizan como medio de transmisión cable coaxial, bifilar o par trenzado, así como el de fibra óptica.

Asimismo, se utiliza el medio inalámbrico, que usa ondas de radio, microondas o infrarrojos, y del cual hablaremos en el capítulo tres.

Cualquier medio, ya se o no físico, que sea capaz de transportar información en forma de señales electromagnéticas, se puede utilizar en redes locales como medio de transmisión.

Las líneas de transmisión son la espina dorsal de la red, ya que a través de ellas se transmite la información entre los distintos terminales (nodos).

Para llevar a cabo la transmisión de la información, se utilizan varias técnicas, pero las más comunes son la banda base y la banda ancha (descritos anteriormente).

Los diferentes tipos de red pueden utilizar distintos tipos de cable y protocolos de comunicación.

1.7.1 Cable coaxial

Hasta hace poco, era el medio de transmisión más común en las redes locales. Consiste en dos conductores concéntricos, separados por un dieléctrico y protegido del exterior por un aislante.

La estructura básica de un cable coaxial se muestra en la figura 1.13

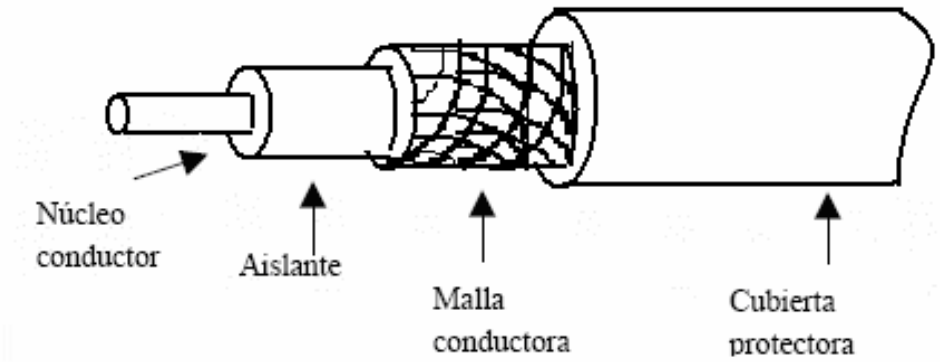


Figura 1.13 Estructura del cable coaxial

1.7.2 Cable bifiliar o par trenzado

El cable de par trenzado consta como mínimo de dos conductores aislados y trenzados entre ellos y protegidos con una cubierta aislante.

Habitualmente, este cable contiene uno, dos o cuatro pares; esto es, dos, cuatro u ocho hilos.

Este cale es económico y fácil de instalar, con conexiones confiables. No obstante, tiene una gran atenuación de láxenla en razón proporcional a la distancia. Es decir, cuanto mayor sea la distancia, mayor será también la interferencia.

La estructura básica de este cable se observa en la figura 1.14

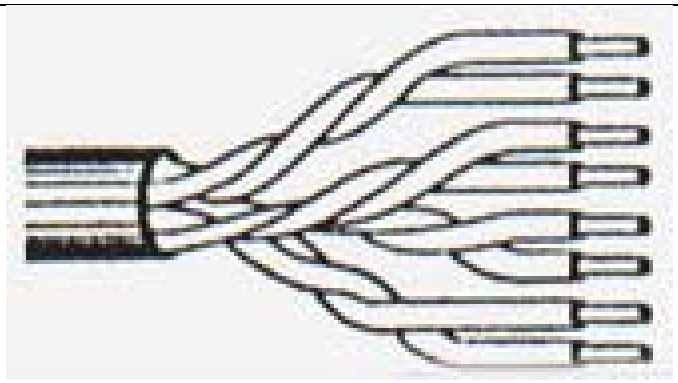


Figura 1.14 Cable de par trenzado

1.7.3 Fibra óptica

La fibra óptica es el medio de transmisión más moderno, utilizado cada vez con mayor frecuencia en redes.

En este medio, las señales de datos son transmitidos a través de impulsos luminosos y pueden recorres grandes distancias (hablando de kilómetros) sin que se tenga que amplificar la señal.

Por su naturaleza, este tipo de señal y cableado es inmune interferencias electromagnéticas, y por su gran ancho de banda, permite transmitir grandes volúmenes de información a alta velocidad.

La estructura básica de la fibra óptica se observa en la figura 1.15

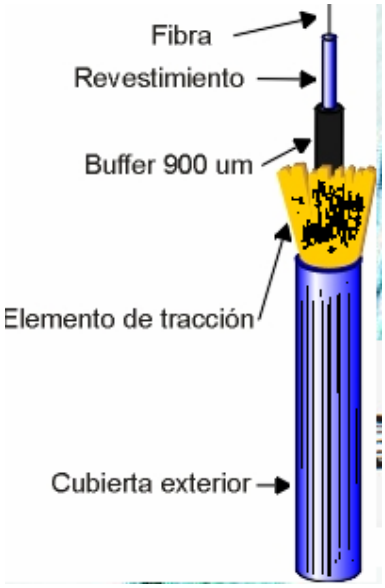


Figura 1.15 Fibra óptica

1.8 Módem

El módem es un periférico que, con el tiempo, se ha convertido en indispensable y pocos son los modelos de ordenador que no estén conectados en red que no lo incorporen.

Su gran aplicación viene dada por dos motivos:

- Internet
- Fax

Aún cuando se le puede dar otros usos (como contestador automático, por ejemplo), para conectarnos con una red local.

Cabe hacer mención de que la principal función de un módem es modular y demodular la señal digital proveniente del ordenador y convertirlo a una forma de onda que sea asimilable por líneas analógicas.; y es utilizado por la red para conectarse a otras redes o a Internet; en este caso, estando conectado a un servidor o un router.

La palabra módem está formada por las raíces de las palabras modulador y demodulador; el modulador es el encargado de recoger las señales digitales y convertirlas en señales analógicas capaces de ser transmitidas por líneas telefónicas.

El demodulador es el que realiza la operación inversa; es decir, transforma las señales analógicas en digitales, capaces de ser utilizadas por la computadora.

1.8.1 Tipos de modulación

La modulación de la señal que emiten los módems puede hacerse de tres maneras:

- Por amplitud.
- Por frecuencia.
- Por fase.

- Modulación por amplitud. En este tipo de modulación, a cada valor de la señal de entrada (sea 1 o 0), se le hace corresponder un valor distinto de la amplitud de la onda portadora.

- Modulación por frecuencia. La modulación por frecuencia consiste en variar la frecuencia de la portadora en función de la señal de entrada, manteniendo la misma amplitud.

- Modulación por fase, La modulación por fase es la variación de la fase de la portadora (normalmente 180°) en función de la señal de estrada.

Además, el módem puede realizar funciones de control y transmisión de datos.

1.8.2 Tipos de módems

El aspecto físico de un módem podría ser el mostrado en la figura 1.16.

Figura 1.16 Vista de un módem de referencia

De acuerdo a su aspecto físico, existen tres tipos de módems:

- Internos
- Externos
- De tarjetas PCMCIA.

Los internos son placas de circuito impreso que se instalan dentro del ordenador. Un ejemplo de módem interno de muestra en la figura 1.17:

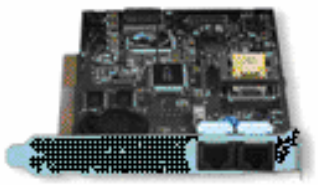


Figura 1.17 Vista de un módem interno

Los externos son pequeñas cajas que se conectan al puerto serie del ordenador, a la red telefónica fija y a la red eléctrica, a través de un alimentador. Esto se observa en la figura 1.18:

Figura 1.18 Vista física de un módem externo

Los módems de tarjeta se insertan en una ranura específica (PCMCIA) de un computador portátil, o en una unidad equivalente para un ordenador de sobremesa. Estos dispositivos toman la alimentación del interior del ordenador, por lo que no requieren de una alimentación aparte.

Un ejemplo de módem de tarjeta se observa en la figura 1.19.

Figura 1.19 Vista física de un módem de tarjeta

Este último es posiblemente el más utilizado, a pesar de que la competencia de los modelos basados en USB es cada vez más fuerte.

1.9 Dispositivos de interconexión para redes alámbricas

Para que una red se comunique, es necesario el uso de conmutadores y/o conectores que permiten la transmisión de datos.

1.9.1 Gateways

Los gateways o pasarelas, son ordenadores o dispositivos que interconecta redes que tienen poco o nada en común entre ellas.

Estos dispositivos trabajan en el nivel de aplicación, y son capaces de traducir información de una aplicación a otra. Tratándose de una red LAN, los gateways son en realidad, routers.

1.9.2 Bridges

Un bridge o puente, es un hardware o software que une dos segmentos lógicos de una misma red física; es decir, divide una red en dos subredes lógicas. En ocasiones se dice que conecta dos redes locales.

El uso de bridges, aisla el tráfico de información innecesaria entre segmentos, de forma que reduce las colisiones.

Los puentes pueden ser locales o remotos; Los puenetes locales son los que conectan redes de un mismo edificio, usando conexiones tanto internas como externas. Los remotos llevan a cabo la conexión a través de redes públicas.

1.9.3 Router

Un router o encaminador, es un conmutador de paquetes que opera en el nivel de red del modelo OSI. Sus características básicas son:

- Permiten interconectar tanto redes de área local (LAN) como redes de área extensa (WAN).
- Proporcionan un control de tráfico y funciones a nivel de red; es decir, trabajan con direcciones de nivel de red (direcciones IP, por ejemplo).
- Trabaja a nivel de red del modelo OSI de la ISO, trabajando con direcciones IP.
- Es dependiente de los protocolos.
- Permite interconectar redes tanto de área local LAN como de área extensa WAN. aunque habitualmente se usa para conectar una LAN a una WAN.
- Son capaces de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo.

Funcionan de la siguiente manera:

Cuando llega un paquete a un router, éste examina la dirección destino y lo envía a través de una ruta predeterminada. Si la dirección destino pertenece a una de las redes que el router interconecta, envía el paquete directamente a ella; en otro caso, enviará el paquete hacia otro router más próximo a la dirección de destino.

Para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento, que funcionan de forma similar a las tablas de los bridges.

1.9.4 Hub y switches

Todos los ordenadores de red están conectados a un concentrador (hub o switch) que sirve de punto de unión de la red.

Este conmutador se encarga de distribuir los paquetes de datos desde el origen hasta el destino. Dicho de otra forma, un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de la red.

1.10 Modelo OSI

Es difícil hablar de redes informáticas sin tocar el punto del modelo OSI (el estándar), en el que se basa su diseño y funcionamiento.

Sabemos que una de las necesidades más importantes de un sistema de comunicaciones es el establecimiento de estándares, sin ellos sólo podrían comunicarse entre sí equipos del mismo fabricante y que usaran la misma tecnología.

La conexión entre equipos electrónicos se ha ido estandarizando paulatinamente siendo la redes telefónicas las pioneras en este campo.

Por ejemplo la histórica CCITT definió los estándares de telefonía: PSTN, PSDN e ISDN.

Otros organismos internacionales que generan normas relativas a las telecomunicaciones son: ITU-TSS (antes CCITT), ANSI, IEEE e ISO

La ISO (International Organisation for Standarisation, Organización internacional de estándares) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos; en detalle, se podría describir como sigue:

- Nivel 1 (Físico) - Se ocupa de la transmisión del flujo de bits a través del medio. - Cables, tarjetas y repetidores (hub).RS-232, X.21.

- Nivel 2 (Enlace) - Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos. - Puentes (bridges). HDLC y LLC.

- Nivel 3 (Red) - Establece las comunicaciones y determina el camino que tomarán los datos en la red. - Encaminador(router). IP, IPX.

- Nivel 4 (Transporte) - La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente. - Pasarela (gateway). UDP, TCP, SPX.

- Nivel 5 (Sesión) - Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones). – Pasarela

- Nivel 6 (Presentación)- Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes. - Pasarela. Compresión, encriptado, VT100.

- Nivel 7 (Aplicación)- Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero). - X400

Estos niveles se observan mejor en la figura 1.20:

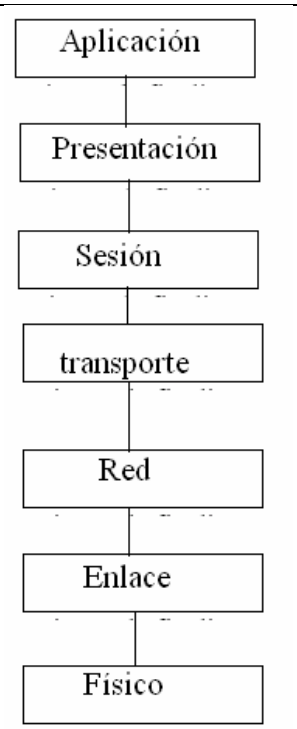


Figura 1.20 Niveles del sistema OSI

La comunicación según el modelo OSI siempre se realizará entre dos sistemas.

Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7.

En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas datos de control.

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir.

La forma, pues de enviar información en el modelo OSI tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Lo anterior se muestra gráficamente en la figura 1.21:

Emisor	Paquete	Receptor
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

Figura 1.21 Comunicación en el sistema OSI

Donde: C7-C2 : Datos de control específicos de cada nivel.

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos protocolos.

Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

CAPÍTULO 2:

REDES COMUNES

CAPITULO 2

REDES COMUNES

2.1 Introducción

Las redes de ordenadores pueden componerse de un mínimo de dos computadores; en ocasiones, estas redes se conectan a otras redes para tener más acceso a información, compartir elementos tanto de información como de dispositivos a larga distancia.

Las redes informáticas han representado una gran ventaja en el manejo de la información a través del tiempo y, nuestros días, siguen asombrando a todos.

2.2 Tipos de redes comunes

La red informática más común es la llamada Internet; con sus variantes de Extranet, cuando es una red abierta; Intranet cuando se trata de una red privada; Ethernet, como manejo de información a través de grandes distancias.

Como sabemos, una red puede ser LAN si es local, WAN si es remota, también puede ser inalámbrica.

2.2.1 Internet

Se puede definir a Internet como una "red de redes"; es decir, que conecta ordenadores y redes de ordenadores al mismo tiempo, de manera que pueda haber una comunicación fácil y rápida a grandes y a cortas distancias.

Las redes de computadoras se comunican a través de algún medio, ya sea cable coaxial, fibra óptica, radiofrecuencia, o alguna otra.

Cabe mencionar que la Internet puede ser manejada e ingresada por medio de redes alámbricas (cableadas) e inalámbricas, sin problema alguno.

En un sentido más técnico, se puede decir que Internet es una combinación de hardware y software. Es una infraestructura de redes a escala mundial que conectan a la vez a todos los tipos de ordenadores.

Una vista general de Internet podría ser como la mostrada en la figura 2.1:

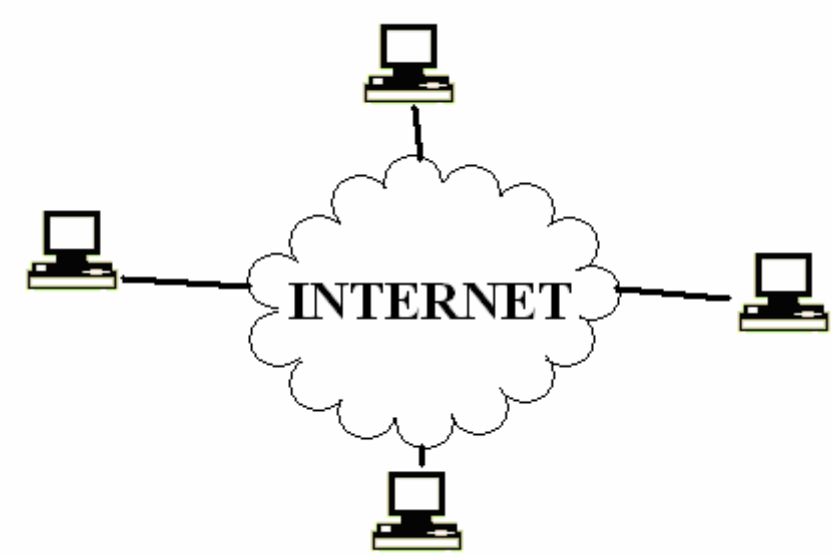


Figura 2.1 Estructura básica de Internet

2.2.1.1 Protocolos de Internet

La red global de Internet se caracteriza porque utiliza un lenguaje común que garantiza la comunicación de los diferentes usuarios; este lenguaje común recibe el nombre de protocolo.

Aún cunado el número de usuarios de Internet sigue creciendo, un número aproximado de seis millones de ordenadores utilizan Internet en todo el mundo; éstos utilizan varios formatos y protocolos, entre los que podemos mencionar:

- Internet Protocol (IP). Se utiliza para dirigir un paquete de datos desde su fuente hasta su destino a través de Internet.
- Transport Control Protocol (TCP). Es de control de transmisión, que se utiliza para la administración de los accesos a la red.
- User Datagram Protocol (UDP). Protocolo del datagrama del usuario, el cual permite enviar un mensaje desde un ordenador a una aplicación que se ejecuta en otro ordenador.

2.2.1.2 Un poco de historia

En los últimos tiempos, Internet se ha convertido en una herramienta básica e indispensable en muchos de los ámbitos de la sociedad; Sin embargo, no es algo nuevo.

Aunque hay muchas versiones acerca del origen de Internet, algunos autores coinciden en que nació en los años sesentas.

En 1968, en Inglaterra, después de varios experimentos, el Laboratorio Nacional de Física de la Gran Bretaña estableció la primera red informática experimental.

Un año después, en el tiempo de la Guerra fría, Estados Unidos crea una red exclusivamente militar; su objetivo de poder acceder a la información militar desde cualquier punto del país, en caso de un ataque ruso. Esta red nace en 1969 y recibe el nombre de ARPANET (Advanced Research Projects Agency NETwork).

Una visión más gráfica del primer proyecto de red informática se puede observar en la figura 2.2:

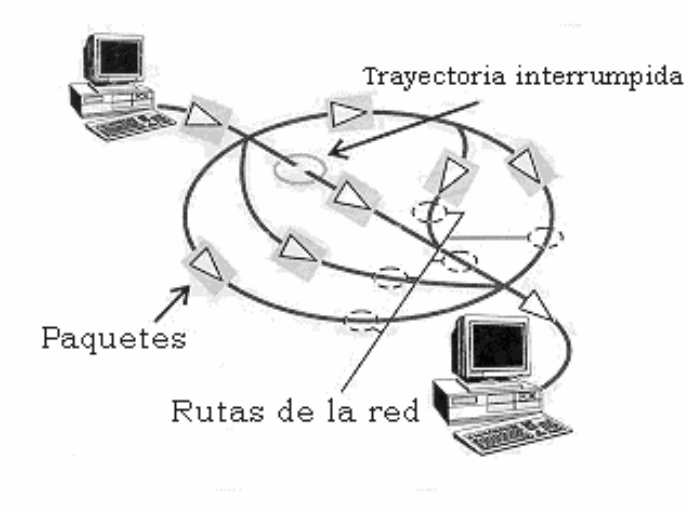


Figura 2.2 Visión del proyecto ARPANET

Como se observa en la figura 2.1, el proyecto contemplaba la eliminación de cualquier tipo de "autoridad central", la razón fue que deseaban evitar el marcar un punto de ataque.

El envío de datos debía ser por paquetes (pequeñas porciones de información) que contendrían la dirección de destino. Si el camino era desviado, el "paquete" buscaría la manera de encontrar el camino de llegada utilizando las vías disponibles.

ARPANET marcó desde el principio, la evolución de las redes de ordenadores, puesto que en la actualidad, los rasgos fundamentales de este proyecto se encuentran presentes en lo que hoy conocemos como Internet.

2.2.1.3 Características de Internet

Internet tiene muchas características que la definen; entre las principales encontramos:

- Se extiende por todo el mundo.
- Es fácil de usar.
- Se puede encontrar, prácticamente, todo tipo de información.
- Es económica en relación al costo que implicaría ir a bibliotecas y tiendas.
- Es útil
- Ofrece una gran libertad de manejo y comunicación.
- Es anónima y confidencial.
- No tiene un dueño, por lo que se dice que es autorreguladora.
- Es un poco caótica.
- Tiene un grado de inseguridad, ya que la información puede ser interceptada.
- Crece vertiginosamente.

Si necesitáramos dar una versión más compacta de las características de Internet, podríamos decir que existen dos características que merecen destacarse:

La inmensidad de información y recursos que hay disponibles; los cuales son constantemente ampliados y/o modificados.

Ausencia de un Administrador Central que tenga control sobre la red o que establezca las normas que deben seguirse para ordenar la información o regular los contenidos; en su lugar existe un grupo de usuarios identificados como ISOC (Internet Society) que cumple con dichas funciones.

Cabe mencionar que cada red que se une a Internet es libre de decidir sus políticas. Cada institución que permite el acceso a cierta información o recursos en sus ordenadores, tiene derecho de decidir qué servicios brinda al resto de la comunidad y de modificarlos cuando lo desee o lo crea necesario.

2.2.1.4 Ventajas de Internet

Internet es la red de ordenadores más utilizada en el mundo; la razón, es que ofrece ventajas importantes, tales como:

- Permanencia en contacto con amigos, sin importar la ubicación en el mundo.
- Discusión abierta a cualquier tema.
- Exploración y búsqueda en millares de bibliotecas y bases de datos globales alrededor del mundo.
- Acceso a millares de documentos, periódicos, revistas y programas.
- Acceso a juegos en vivo y en tiempo real; permite jugar con docenas de personas de inmediato.
- Servicio de noticias de cualquier tipo.
- Permite la ampliación del conocimiento para quien está dispuesto a aprendes
- Provee de guías sobre su propio uso para usuarios nuevos en el uso de la red.

2.2.1.5 Desventajas de Internet

Como todo sistema, ya sea o no informático, el Internet tiene desventajas de acuerdo a su uso y por su manejo.

Una de los principales inconvenientes es hacia los niños, si no existe una restricción para el acceso de páginas prohibidas (xxx, drogas, etcétera).

Hoy en día, los juegos de video a través de Internet ha provocado que muchos niños y jóvenes permanezcan frente a sus computadoras sin importarles lo que pase en su alrededor, se convierten en personas aisladas y calladas.

Un riesgo de Internet se da en la educación, en donde los estudiantes han olvidado leer y consultar y sólo copian la información en la red; esto provoca un déficit en materia de atención y educación, puesto que nunca se enteran de qué es lo que escriben y se acostumbran a “no pensar”, lo que trae consecuencias a largo plazo.

2.2.2 Intranet

Se puede definir a Intranet como una red derivada de Internet, basada en los mismos estándares de ésta y con la principal característica de ser únicamente privada.

Las Intranets utilizan tecnologías de Internet para enlazar los recursos informativos de una organización, desde documentos de texto hasta multimedia; desde bases de datos legales hasta sistemas de gestión de documentos.

Una Intranet puede contener sistemas de seguridad para la red, tablones de anuncios y motores de búsqueda; puede extenderse a través de Internet; Generalmente, esto se logra usando una red privada virtual (VPN).

La estructura básica de Intranet se puede observar en la figura 2.3:

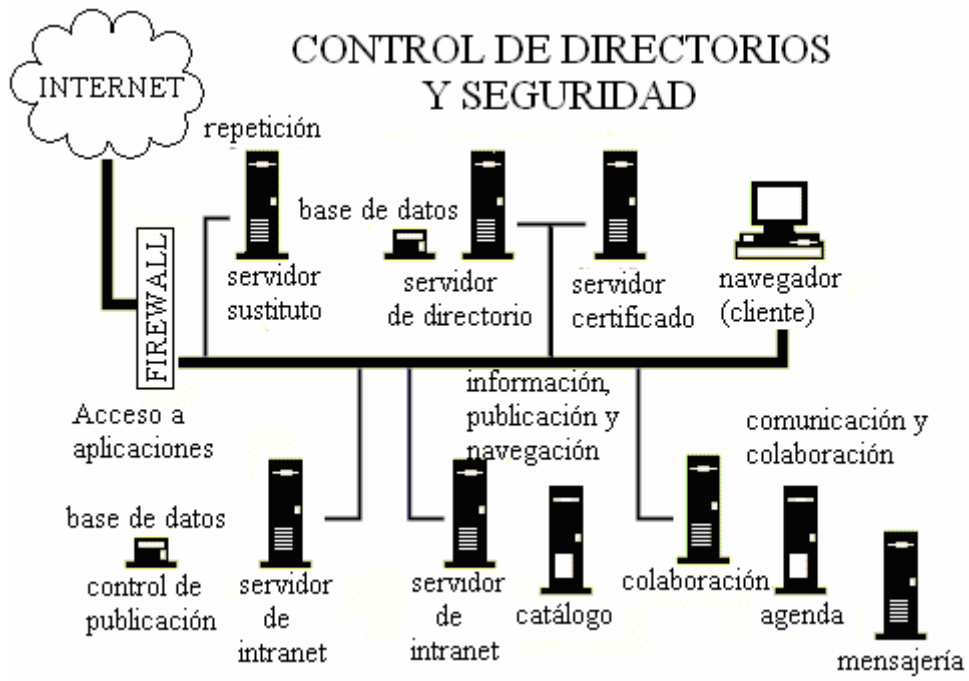


Figura 2.3 Estructura de una Intranet

2.2.2.1 Protocolos de Intranet

Como se dijo anteriormente, una Intranet es una red privada derivada de Internet y maneja sus características y también los protocolos TCP/IP. Esta red puede o no, tener salida a Internet. En el caso de que sí cuente con ésta, el direccionamiento IP permite la salida de las direcciones privadas, pero impide el acceso desde Internet.

Lo anterior se puede observar en la figura 2.4:

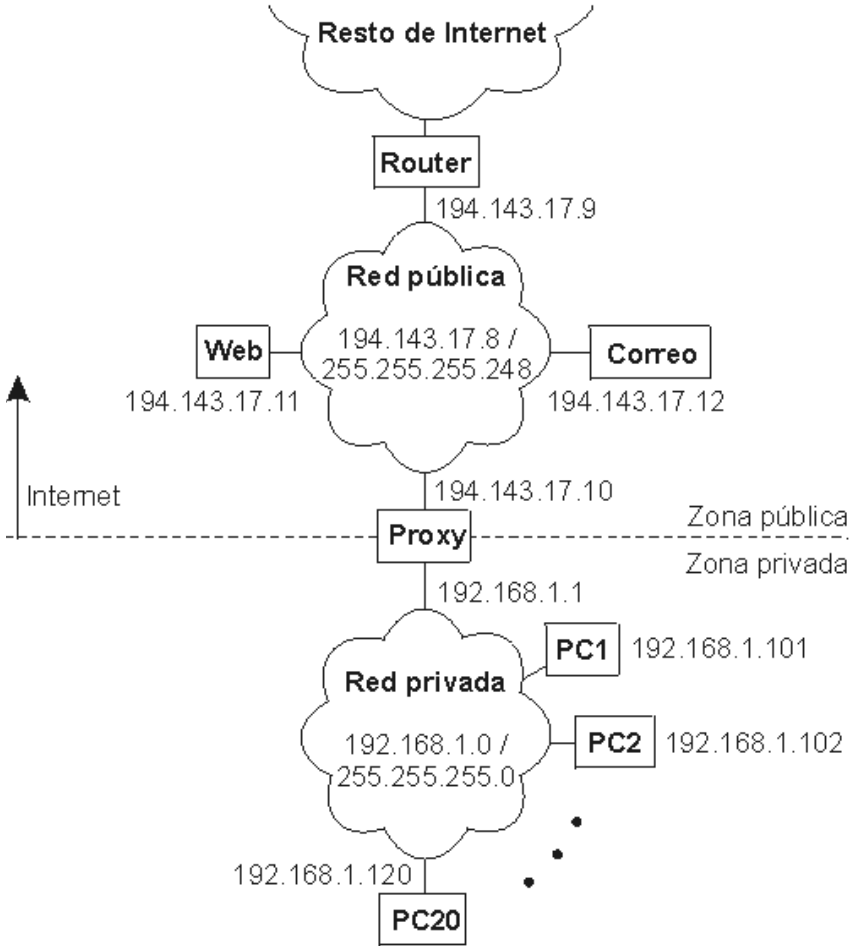


Figura 2.4 Vista de trabajo de una Intranet

2.2.2.2 Intranet a través del tiempo

Intranet nace hace relativamente poco tiempo; surge de la necesidad de las empresas en la privacidad de su información.

Intranet es una red privada en donde la información que circula puede únicamente ser accedida por el personal registrado y tiene restricciones para usuarios no autorizados.

2.2.2.3 Características de Intranet

Uno de los aspectos más destacados de la Intranet es la seguridad de la información. Para que solamente los miembros de una organización puedan acceder a la información, cualquier conexión que no tenga una autorización debe ser automáticamente bloqueada, con el fin de evitar accesos indeseados y/o fuga de información importante.

Así, las características básicas que definen a Intranet son:

- Totalmente basada en Web
- Foros internos de discusión según temáticas.
- Carpetas para todos los temas relevantes.
- Determina códigos de acceso según niveles de seguridad.
- Crea lugares para publicar notas, artículos, opiniones, etcétera.
- El administrador determina a las personas que tienen acceso a la información, previo convenio o instrucción de quien origina ésta.
- Facilita y agiliza la realización de encuestas internas.
- Mantiene políticas específicas de seguridad.
- Calendario personal.
- Agenda de contactos; es decir, base de datos sobre los contactos de la empresa.
- Publica eventos destacados, novedades, etcétera.

2.2.2.4 Ventajas de Intranet

Intranet ofrece ciertas ventajas en su manejo, lo que influye en su implantación; entre éstas podemos destacar las siguientes:

- Es una forma muy eficiente y económica de distribuir la información interna, sustituyendo los medios clásicos.
- Fácil adaptación y configuración a la infraestructura tecnológica de la organización, así como gestión y manipulación. Disponible en todas las plataformas informáticas.
- Adaptación a las necesidades de diferentes niveles: Empresas, departamentos, áreas de negocios, etcétera. Centraliza el acceso a la información actualizada de la organización, al mismo tiempo que puede servir para organizar y acceder a la información de la competencia dispuesta en Internet.
- Sencilla integración de multimedia
- Posibilidad de integración con las bases de datos internas de la organización en particular.

- Rápida formación del personal.
- Acceso a Internet.
- Uso de estándares públicos y abiertos, independientes de empresas externas.

2.2.2.5 Desventajas de Intranet

Los principales inconvenientes del uso de una Intranet son:

- No se puede poner en marcha si no se conocen las necesidades específicas, tanto de la Intranet como del personal a cargo.
- Las Intranets son redes expuestas a notables riesgos de seguridad.

2.2.3 Extranet

Una Extranet es una red de ordenadores interconectados que utiliza los estándares de Internet. El acceso a esa red está restringido a un determinado grupo de empresas y organizaciones independientes que necesitan trabajar de manera coordinada para ahorrar tiempo y dinero en sus relaciones de negocios.

2.2.3.1 Composición de Extranet

Se puede decir que una Extranet es la unión de dos Intranets.

Esta relación se marca en la figura 2.5.

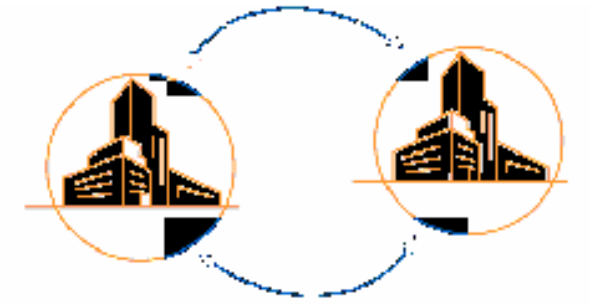


Figura 2.5 Estructura básica de una Extranet

3.2.3.2 Uso de Extranet

Una Extranet es adecuada para aquellas empresas que tienen la necesidad de comunicarse datos confidenciales entre ellas y el utilizar la tecnología de Internet supone un importante ahorro de tiempo y dinero.
La seguridad en el diseño de la Extranet es fundamental para asegurar que los datos confidenciales lo sigan siendo pese a viajar por la red; que sólo personas autorizadas tengan acceso a la información de las empresas en cuestión.

La comunicación de las Extranet se muestra en la figura 2.6

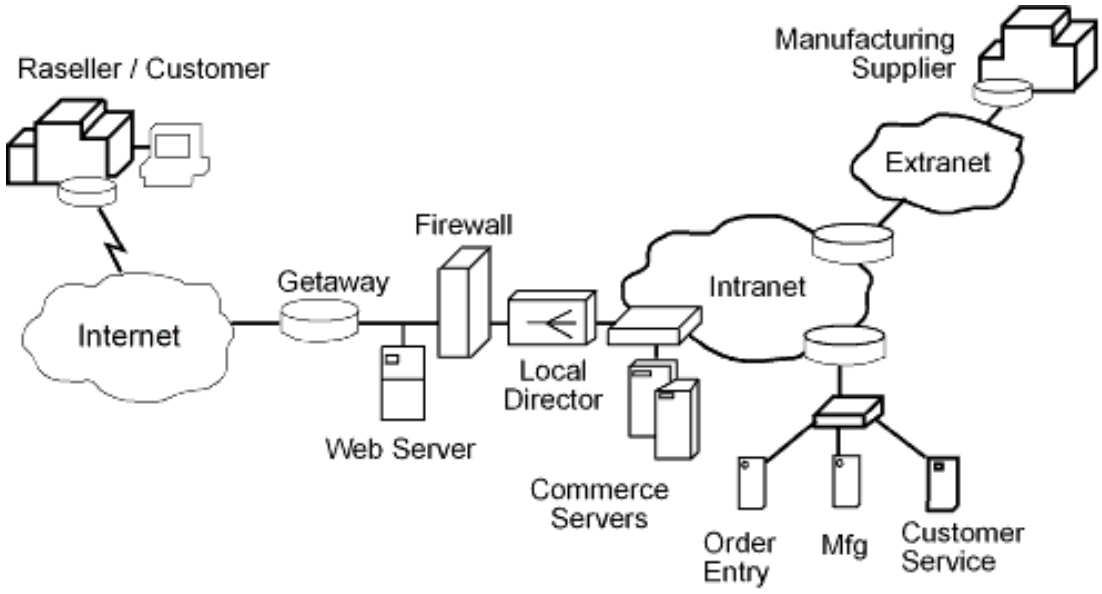


Figura 2.6 La comunicación de Extranet

2.2.3.3 Ventajas de Extranet

Una empresa podrá ir abriendo sus archivos de información a sus proveedores y clientes con el ahorro que esto supone:

- Consultas on-line de pedidos.
- Consultas de niveles de stock.
- Consultas de condiciones compra/venta
- Introducción de incidencias.
- Comunicaciones.

- Formación on-line
- Etcétera.

Cabe mencionar que Extranet se puede implantar de manera modular.

2.2.4 Ethernet

Ethernet es la tecnología de red de área local (LAN) más extendida en la actualidad. Es una red de banda base; es decir, provee un único canal de comunicación sobre el medio físico (cable), de manera que sólo un dispositivo puede utilizarlo a la vez.

Su funcionamiento se basa en tramas de datos; y ha sido aceptada como estándar por la IEEE.

La tecnología define las características de cableado y señalización del nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.

En su concepción, Ethernet era visto de una manera muy ambiciosa; el boceto que muestra lo anterior se ve en la figura 2.7

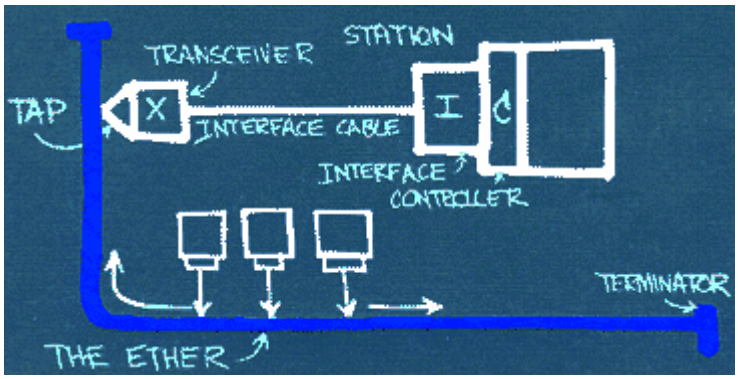


Figura 2.7 Primer boceto de Ethernet

2.2.4.1 Características de Ethernet

Muchas son las características que definen a Ethernet; algunas de la cuales se listan a continuación:

- Sus especificaciones (IEEE 802.3) han sido adoptadas por ISO y se encuentran en el estándar internacional 8802-3.

- Está basado en la lógica de la topología de bus. En su origen, el bus era una longitud única de cable a la cual los dispositivos de red estaban conectados. En la actualidad, el bus se ha miniaturizado y puesto en un concentrador (hub) al cual las estaciones, servidores y otros dispositivos son conectados.

- Utiliza un método de acceso al medio por disputa (contention). Las transmisiones son difundidas en el canal compartido para ser escuchadas por todos los dispositivos conectados, pero solamente el dispositivo de destino provisto es el que va a aceptar la transmisión. Este tipo de acceso se conoce como CSMA/CD.

- Ha evolucionado para operar sobre una variedad de medios: Cable coaxial, Par trenzado y fibra óptica; a múltiples tasas de transferencia.

- Todas las implementaciones son interoperables, lo que simplifica el proceso de migración a nuevas versiones de Ethernet.

- Múltiples segmentos de Ethernet pueden ser conectados para formar una gran red LAN Ethernet utilizando repetidores. La correcta operación de este tipo de red depende de que los segmentos del medio sean construidos de acuerdo a las reglas para este tipo de medio. Las relas incluyen límites en el número total de segmentos y repetidores que pueden ser utilizados en la construcción de una LAN.

- Fue diseñado para ser expandido con facilidad.

- El uso de dispositivos de interconexión como: Bridges (puentes), routers (ruteadores), switches (conmutadores); permiten que redes LAN individuales se conecten entre sí. Cada LAN continúa operando en forma independiente pero es capaz de comunicarse fácilmente con las otras LANs conectadas.

2.2.4.2 Historia de Ethernet

El año 1972 fue marcado para el inicio del desarrollo de una tecnología de redes llamada Ethernet Experimental.

El sistema desarrollado, conocido en ese momento como red ALTO Aloha; fue la primera red de área local para computadores personales (PCs). Esta red funcionó por primera vez en mayo de 1973, a una velocidad de 2.94 Mb/s.

Las especificaciones formales de Ethernet fueron desarroladas por Xerox, Digital (DEC) e Intel, y se publicó en el año de 1980. Tales especificaciones son conocidas como el estándar DEC-Intel-Xerox (DIX): el Libro Azul de Ethernet. Este documento hizo de Ethernet Experimental un estándar abierto.

La tecnología Ethernet fue adoptada para su estandarización por el Comité de Redes Locales (LAN) de la IEEE como IEEE 802.3. Este estándar fue publicado por primera vez en 1985.

El estándar IEEE 802.3 provee un sistema tipo Ethernet basado (aunque no idéntico) en el estándar DIX original. El nombre correcto de esta tecnología es IEEE 802.3 CSMA/CD, pero regularmente es referido como Ethernet.

IEEE 802.3 Ethernet fue adoptada por la Organización Internacional de Estandarización (ISO), haciendo de él un estándar de redes internacional.

En respuesta a los cambios en la tecnología y las cambiantes necesidades de los usuarios, Ethernet continuó evolucionando.

Desde 1985, el estándar IEEE 802.3 se actualizó para incluir nuevas tecnologías. Por ejemplo:

- El estándar 10BASE-T fue aprobado en 1990,
- El estándar 100BASE-T fue aprobado en 1995 y
- Gigabit Ethernet sobre fibra fue aprobado en 1998.

En el presente texto, no profundizaremos en este tipo de tecnologías.

2.2.4.3 Ventajas de Ethernet

Son muchas las ventajas del nivel del Protocolo de Control e Información (CIP) sobre Ethernet/IP:

- La oferta de un acceso consistente en aplicaciones físicas significa que se puede utilizar una sola herramienta para configurar dispositivos CIP en distintas redes desde un único punto de acceso sin la necesidad de software propietario.
- Al clasificar todos los mecanismos como objetos o elementos, se reduce la necesidad de adiestramiento y los costos de puesta en marcha requeridos cuando se incorporan nuevos mecanismos al perímetro de la red.
- Ethernet/IP disminuye el tiempo de respuesta e incrementa la capacidad de transferencia de datos respecto a otros protocolos (como DeviceNet o ControlNet).
- A través de un mismo medio de interconexión, Ethernet/IP conecta distintos mecanismos industriales con el control de planta y con la gestión central, mediante una interfaz consistente con las aplicaciones

2.2.4.4 Desventajas de Ethernet

Como todo sistema, un cable delgado de Ethernet tiene algunas desventajas:

- Dado que no proporciona mucha protección contra la interferencia eléctrica, el cable delgado Ethernet no puede ser colocado junto a un equipo eléctrico potente (por ejemplo, en una fábrica).
- El cable delgado Ethernet cubre distancias más cortas y soporta un menor número de conexiones de computadoras por red que el cable grueso Ethernet.
- El uso del cable grueso de Ethernet supone un incremento en los costos de implantación.

2.2.5 Red de área local (LAN)

LAN es la abreviatura de Locar Area Network (Red de Área Local o simplemente, Red Local).

Una red local es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un entorno de unos pocos kilómetros, como puede ser una oficina o un edificio.

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

El término Red Local incluye tanto el hardware como el software necesario para la interconexión de los diferentes dispositivos y el tratamiento de la información.

El esquema de una red de área local se ilustra en la figura 2.8:

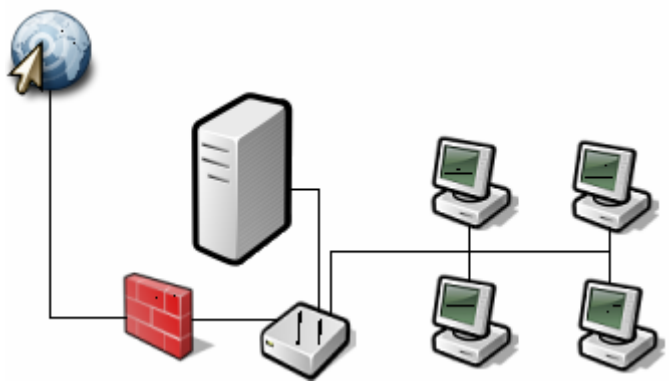


Figura 2.8 Esquema de red de área local (LAN)

2.2.5.1 Evolución de las LANs

En los días anteriores a los ordenadores personales, una empresa podía tener solamente un computador central; los usuarios accedían a esta vía mediante terminales de ordenador sobre un cable simple de baja velocidad.

Las redes como SNA de IBM (arquitectura de red de sistemas), fueron diseñadas para enlazar terminales u ordenadores centrales a sitios remotos sobre líneas alquiladas.

Las primeras Redes de Área Local fueron creadas al final de la década de los setentas y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar. Muchos de los sistema fiables creados en esa época (como Ethernet y ARCNET) fueron los más populares.

El crecimiento CP/M y DOS basados en la computadora personal, permitieron que en un lugar físico existieran docenas e incluso, cientos de ordenadores. La finalidad inicial de conectar estos ordenadores se refirió a compartir espacios en disco e impresoras láser; puesto que estos recursos eran muy costosos.

Había muchas expectativas en este tema desde 1983 en adelante; y la industria informática declaró que el siguiente año sería “El año de las LANs”. Hecho que nunca se dio, debido a la proliferación de las incompatibilidades de la capa física y la implantación del protocolo de red, y la confusión sobre la mejor manera de compartir los recursos. Lo normal era que cada usuario tuviera una tarjeta de red, cableado y protocolo y sistema de operación de red.

Con la aparición de Netware surgió una nueva solución; ésta ofrecía un soporte imparcial para los cuarenta o más tipos que existían de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores.

Netware dominaba el campo de las LANs de los ordenadores personales desde antes de su introducción en 1983 y hasta mediados de los años noventas, cuando Microsoft introdujo Windows NT Advanced Server y Windows for Workgroups.

De todos los competidores de Netware, solamente Banyan VINES tenía fuerza técnica comparable, pero ésta se ganó una base segura. Microsoft y 3Com trabajaron juntos para crear un sistema de operaciones de red simple, el cual estaba formado por la base de 3Com´s+Share, el Gestor de Redes LAN de Microsoft y el Servidos de IBM. Ninguno de estos proyectos fue especialmente satisfactorio.

2.2.5.2 Características de LAN

Las características más notables de las redes LANs son:

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Cableado específico instalado normalmente a propósito.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima de 3 kilómetros.
- Uso de un medio privado de comunicación.
- Simplicidad del medio de transmisión que utiliza: Cable coaxial, cable telefónico, fibra óptica.
- Facilidad para efectuar modificaciones, tanto en el hardware como en el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.

2.2.5.3 Ventajas de redes LAN

Las redes de área local es una solución a muchos problemas en una empresa, como la redundancia de hardware, de datos o de software, entre otros.

Las redes de área local permite:

- Compartir bases de datos, con lo que se elimina la redundancia de datos.
- Compartir programas, lo cual elimina la redundancia de software.
- Compartir periféricos (módem, tarjeta RDSI, impresora, etcétera); con ello se elimina la redundancia de hardware.
- Poner a disposición del usuario medios de comunicación como el correo electrónico y el Chat.
- Realizar un proceso distribuido; es decir, las tareas se pueden repartir en distintos nodos

- La integración de los procesos y los datos de cada uno de los usuarios en un sistema de trabajo corporativo.

- Tener la posibilidad de centralizar la información o procedimientos, lo cual facilita la administración y la gestión de los equipos.

Además, una red de área local implica un importante ahorro; tanto en dinero, puesto que no es preciso comprar gran cantidad de periféricos y en consecuencia, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica compartida por varios computadores; como de tiempo, ya que se logra la gestión de la información y del trabajo.

2.2.6 Redes de cobertura amplia (WAN)

Una red de área amplia, WAN por sus siglas en inglés (Wide Area Network), es una categoría de red de computadoras, capaz de cubrir grandes distancias (100 Km. a 1000 Km. aproximadamente), dando el servicio a un país o a un continente.

Podemos decir que cualquier tipo de red en la que todos los usuarios no se encuentren en un mismo edificio, corresponde a esta categoría de red.

2.2.6.1 Necesidad de redes WAN

Generalmente, las redes de área amplia son construidas bajo especificaciones particulares, y enfocadas a las necesidades de una organización o empresa; y son de uso privado.

En ocasiones, son construidas por los proveedores de Internet para proveer de conexión a sus clientes.

Actualmente, Internet proporciona redes de área amplia de alta velocidad y la necesidad de redes privadas WAN se ha reducido drásticamente; mientras que las VPN (red privada virtual) aumentan continuamente; la razón, es que éstas últimas utilizan cifrado y otras técnicas para hacer esa red dedicada.

2.2.6.2 Estructura de red WAN

Las redes WAN son conformadas por:

- Nodos de conmutación,
- Líneas de transmisión de grandes prestaciones (caracterizadas por sus grandes velocidades y ancho de banda en la mayoría de los casos); también llamadas circuitos, canales o troncales.

La estructura de una red WAN se muestra en la figura 2.9:

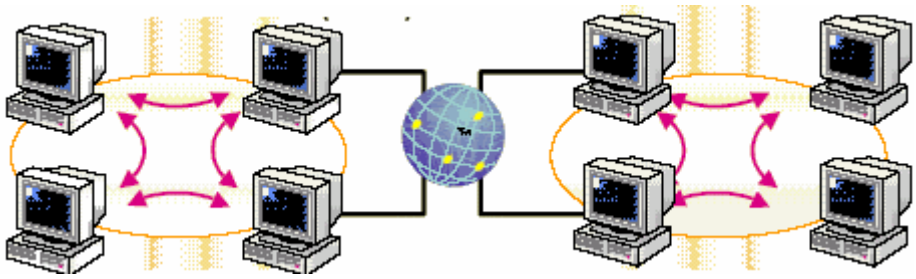


Figura 2.9 Estructura básica de una red WAN

2.2.6.3 Características de una red WAN

Las características que definen una red de área amplia son:

- Posee máquinas dedicadas a la ejecución de los programas de usuario (hosts).
- Una subred, en donde se conectan uno o varios hosts.
- División entre líneas de transmisión y elementos de conmutación (enrutadores).
- Es una solución cuando la red de área local necesita ser ampliada.
- Los canales son proporcionados, regularmente, por las compañías telefónicas.

2.2.6.4 Desventajas de la red WAN

Entre las desventajas de uso de redes WAN, podemos mencionar las siguientes:

- Los canales de comunicación tienen un costo (mensual para línea alquilada, o costo proporcional para línea normal conmutada)
- Los enlaces son relativamente lentos (1200 Kbit/seg a 1.55 Mbit/seg).
- Las conexiones de los ETD con los ECD son, generalmente, más lentas (150 bit/seg a 19.2 Kbit/seg)
- Las líneas son relativamente propensas a errores.
- Su estructura tiende a ser irregular, debido a la necesidad de conectar múltiples terminales, computadores y centros de conmutación.

2.2.7 Redes inalámbricas

Una red inalámbrica es un conjunto de computadoras o dispositivos informáticos, comunicados entre sí mediante soluciones que no requieren el uso de cables de interconexión.

Profundizaremos más sobre las redes inalámbricas en el Capítulo 3.

2.2.7.1 Ventajas de las redes inalámbricas.

Las principales ventajas que ofrecen las redes inalámbricas frente a las cableadas, son:

- Movilidad
- Desplazamiento
- Flexibilidad
- Ahorro de costes
- Escalabilidad

2.2.7.2 Desventajas de las redes inalámbricas

Los principales inconvenientes de las redes inalámbricas son:

- Menor ancho de banda
- Mayor inversión inicial
- Vulnerabilidad a accesos no autorizados.
- Interferencias
- Incertidumbre tecnológica

CAPÍTULO 3:

REDES INALÁMBRICAS

CAPÍTULO 3:

REDES INALÁMBRICAS

3.1 Introducción

La comunicación inalámbrica va avanzando a través del tiempo; diversos fabricantes las han podido incluir en el mercado de consumo con muy buenos resultados.

De una forma callada, las redes inalámbricas o Gíreles Networks (WN) se están introduciendo en el mercado de consumo gracias a unos precios populares y a un conjunto de entusiastas, principalmente particulares, que han visto las enormes posibilidades de esta tecnología.

Algunas de las nuevas tecnologías que han proliferado en los últimos años son:

- WIFI
- WIMAX
- GSM
- Bluetooth
- Infrarrojos (IrDA)

Los dispositivos inalámbricos constituyen una de las grandes revoluciones de este siglo; esto es, en el uso de las tecnologías de la información.

3.2 Características básicas de las redes inalámbricas

La implantación de redes inalámbricas puede ser un tanto engañosa. Parece algo sencillo (aún más que redes cableadas), pero resulta bastante complejo configurarlas de manera óptima, si no se tienen las herramientas adecuadas y sólidos conocimientos al respecto. Más complicado resulta el protegerlas.

Podemos decir que las redes inalámbricas tienen características propias, las más significativas son:

- Son muy fáciles de adquirir.
- Son difíciles de configurar.
- Son sumamente difíciles de proteger.

Lo anterior puede hacer a muchos desistir de su implementación; sin embargo, las redes inalámbricas resultan muy útiles de acuerdo al tipo de trabajo e instalaciones, como veremos más adelante.

3.3 Elementos básicos de una red inalámbrica

Las redes inalámbricas pretenden mucho y están en camino para lograr su objetivo: Ser utilizadas, cada vez más, por un número mayor de personas. Para este fin, se vale de diversos elementos que las componen y permiten satisfacer las necesidades de los usuarios.

Los elementos básicos de una red inalámbrica son:

- Punto de acceso
- Dispositivos móviles
- Dispositivos fijos
- Otros elementos

3.3.1 Punto de acceso

El Punto de Acceso o Access Point, por sus siglas en inglés (AP), es un dispositivo inalámbrico central de una red Wireless, que por medio de ondas de radio frecuencia recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidos de la red cableada; es decir, hace de puente entre la red cableada y la red inalámbrica.

El esquema de funcionamiento de un Punto de Acceso se puede observar en la figura 3.1:

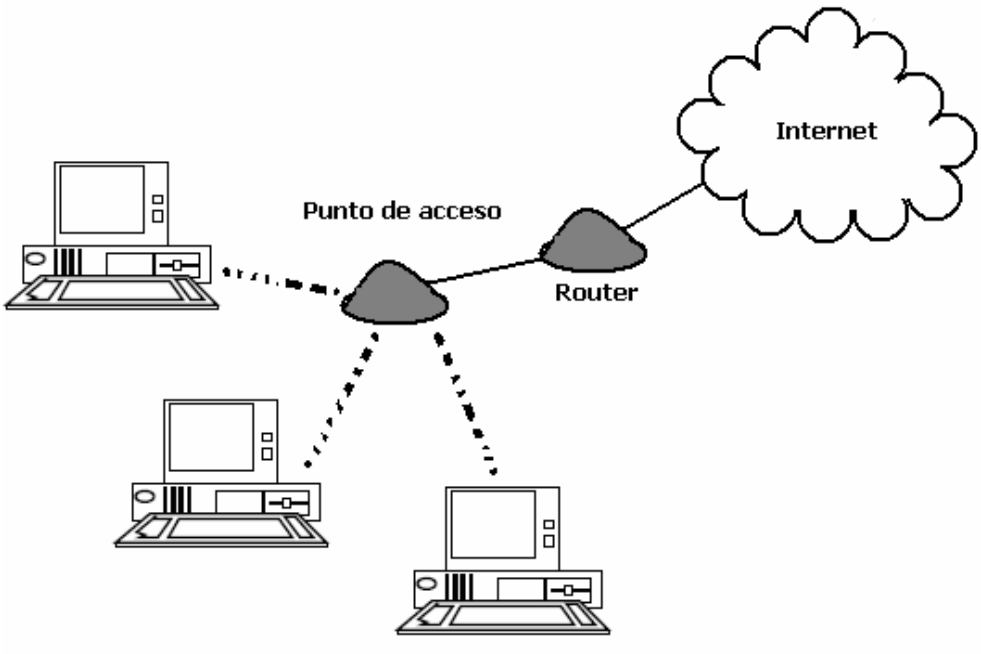


Figura 3.1 Esquema de Punto de Acceso

La vista física de este dispositivo se muestra en la figura 3.2:

Figura 3.2 Apariencia física de un Punto de Acceso

Los puntos de acceso pueden ser de dos tipos: Básicos (Thin) o robustos (Fat), de acuerdo con la cantidad de terminales e información que manejan.

Las características de puntos de acceso robustos son:

- Son bastante inteligentes e incorporan funciones adicionales de seguridad y gestión.
- Son más costosos.
- Son más complicados de gestionar.
- Sobrecargan el tráfico
- En algunos casos, tienen elementos libres para futuras actualizaciones.

Las características de los puntos de acceso básicos son:

- Más económicos.
- Más sencillos de gestionar y configurar.
- Es más fácil compatibilizarlos con otras marcas.

3.3.2 Dispositivos móviles

Hay diversos dispositivos móviles, como: computadores, PDAs, teléfonos celulares.

Generalmente, los dispositivos móviles tienen instalados tarjets PCMCIA o dispositivos USB con capacidades WI-FI y pueden recibir o enviar información a los puntos de acceso o a otros dispositivos de manera inalámbrica.

Actualmente, son innumerables los que tienen la tecnología Wi-Fi incorporada en el procesador; y por tanto, no necesitan de agregados.

La vista física de este tipo de dispositivos, se observa en la figura 3.3:

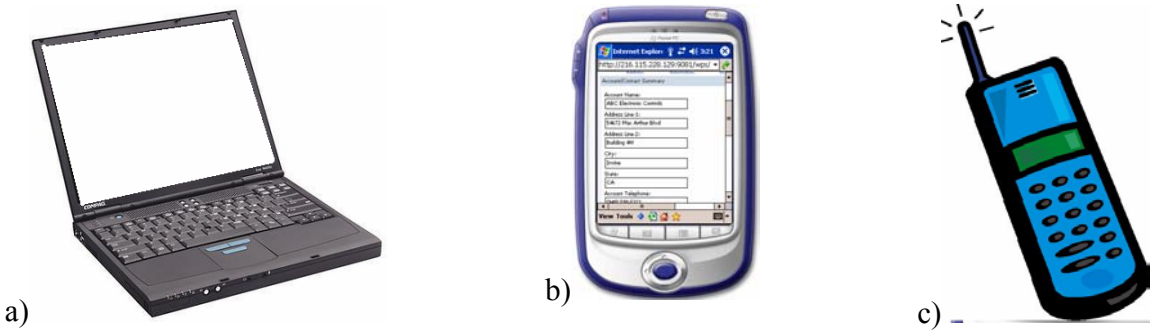


Figura 3.3 Apariencia de dispositivos móviles a) Lap top b) PDA c) Teléfono celular

3.3.3 Dispositivos fijos

Entre los dispositivos fijos podemos encontrar: Computadoras fijas, cámaras de vigilancia, etcétera; que pueden incorporar tecnología Wi-Fi y, por tanto, ser parte de una red inalámbrica.

La vista física de este tipo de dispositivos se muestra en la figura 3.4:

Figura 3.4 Apariencia física de dispositivos fijos a) Computador b) Cámara de vigilancia

3.3.4 Otros elementos

También existen otros elementos como amplificadores y antenas que se pueden agregar, según los requerimientos, a instalaciones inalámbricas, y sirven para direccional y mejorar las señales de radio-frecuencia transmitidas.

3.4 Tipos de redes inalámbricas

Las redes inalámbricas pueden clasificarse de acuerdo con diversos criterios: por la forma en que se pueden conectar, por el tipo de uso, por la distancia en la cobertura de comunicación.

Estos criterios de clasificación de redes inalámbricas se muestran en el cuadro sinóptico de la figura 3.5:

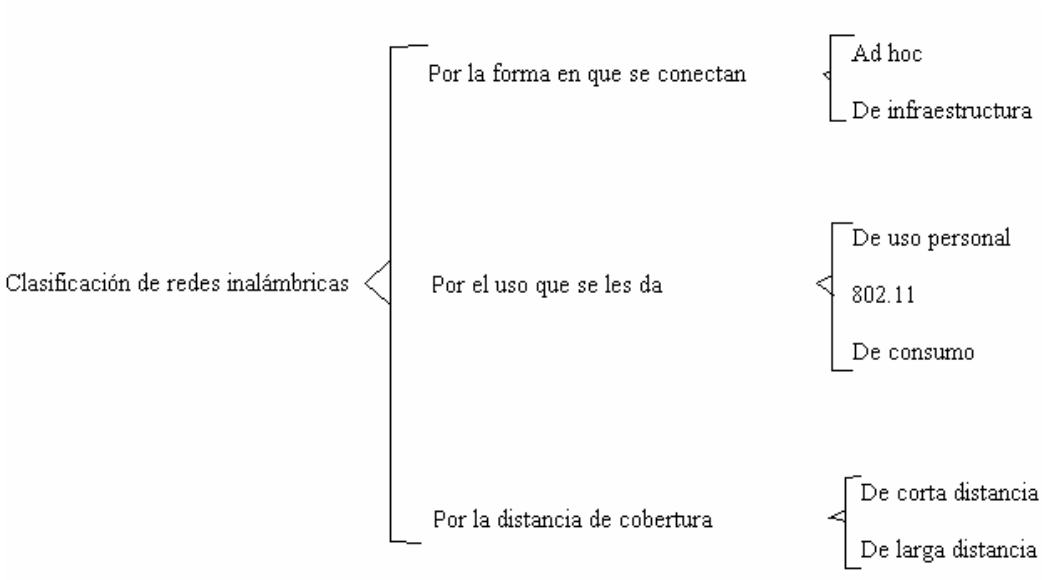


Figura 3.5 Cuadro sinóptico de los criterios de clasificación de archivos

3.4.1 Por la forma en que se conectan

Como vimos, las redes inalámbricas se pueden conectar básicamente de dos formas:

- Ad-hoc
- Infraestructura

En la topología Ad hoc, Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red "de igual a igual"; para ello se necesita disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos, puesto que haría bajar el rendimiento de la red.

Cabe mencionar que a mayor dispersión geográfica de cada nodo, mayor número de dispositivos pueden formar parte de la red, aún cuando algunos no lleguen a verse entre sí.

La figura 3.6 nos muestra un ejemplo gráfico de esta topología:

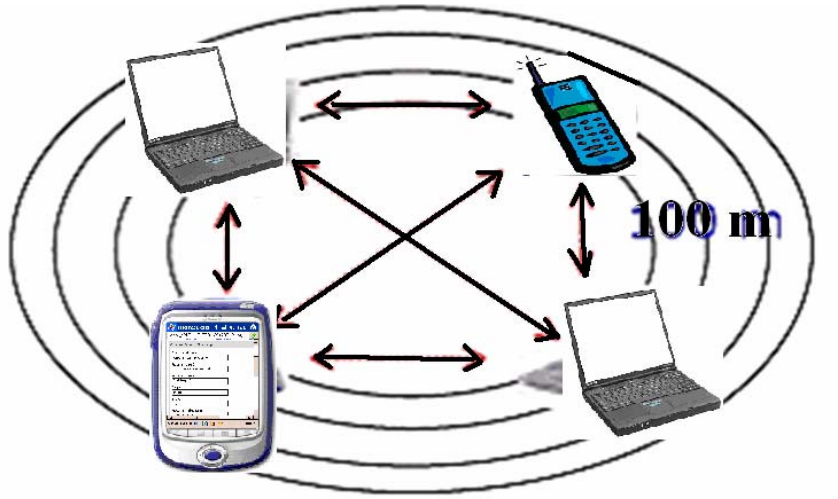


Figura 3.6 Topología Ad hoc

En la topología de Infraestructura, existe un nodo central o Punto de Acceso Wi Fi, que sirve de enlace para todos los demás. Este nodo sirve para encaminar tramas hacia una red convencional o hacia otras redes distintas.

Para poder establecer una comunicación entre los nodos, éstos deben de estar dentro de la zona de cobertura del Punto de Acceso (Access Point).

Lo anterior se muestra en la figura 3.7:

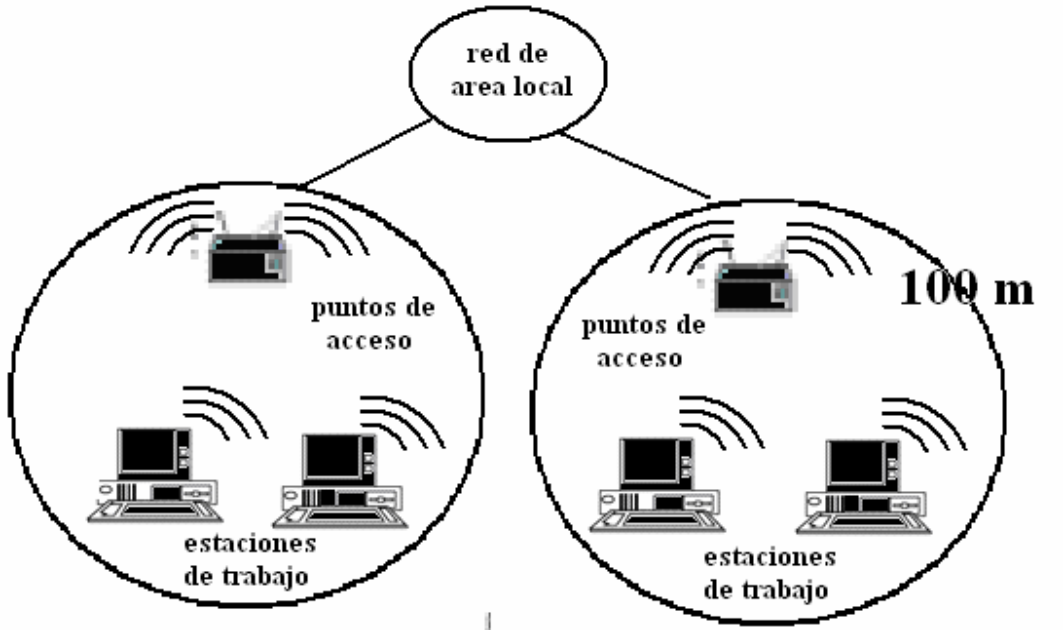


Figura 3.7 Topología de Infraestructura

3.4.2 Por el uso que se les da

El uso y/o el tipo de usuarios de las redes inalámbricas crean otro criterio de clasificación: De uso personal, 802.11 o de consumo.

Dentro del ámbito de las redes inalámbricas de uso personal, se pueden integrar dos elementos básicos:

- En primer lugar, están las redes de uso actual mediante el intercambio de información mediante infrarrojos. Estas redes son muy limitadas debido a su corto alcance, necesidad de "visión de obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 Kbps). Se encuentran principalmente en ordenadores portátiles, Agendas electrónicas personales (PDAs), teléfonos móviles y algunas impresoras.

- En segundo lugar, el Bluetooth, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDA's, teléfonos móviles de nueva generación y algún otro ordenador portátil. Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo se ha plagado de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes; lo cual ha imposibilitado su rápida adopción. Opera dentro del rango de los 2.4 GHz.

Las redes inalámbricas (WN), se diferencian de las redes conocidas por el enfoque que toman de los niveles más bajos de la pila OSI (Organismo de estandarización internacional), el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 de IEEE.

Regularmente, al aparecer nuevos estándares y obtener la atención e interés de grandes fabricantes, aparecen también diferentes aproximaciones al mismo, lo que genera una incipiente confusión.

En este sentido, nos encontramos con tres principales variantes:

- 802.11a
- 802.11b
- 802.11g

Aunque actualmente existen más de éstas.

En las redes inalámbricas de consumo encontramos las redes CDMA y GSM; y las 802.16.

- Las redes CDMA (estándar de telefonía móvil estadounidense) y GSM (estándar de telefonía móvil europeo y asiático), son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.
- Las 802.16 son redes que pretenden complementar a las anteriores, estableciendo redes inalámbricas metropolitanas (MAN's) en el rango de entre los 2 GHz y los 11

3.4.3 Por la distancia de cobertura

Las redes inalámbricas pueden clasificarse de acuerdo a la distancia entre sus nodos en: De corta distancia y De larga distancia.

Generalmente, las redes de corta distancia son utilizadas en redes corporativas cuyas oficinas se encuentran en uno o varios edificios, no muy retirados unos de otros, con velocidades en el rango de 280 Kbps y 2 Mbps.

Las redes de larga distancia son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos; sus velocidades de transmisión son relativamente bajas (4.8 Kbps a 19.2 Kbps).

Dentro de las redes de larga distancia podemos encontrar:

- Redes públicas de conmutación de paquetes.
- Redes privadas de conmutación de paquetes.
- Redes telefónicas celulares.
- Redes de área local.
- Redes infrarrojas.
- Redes de radio frecuencia.

3.5 Ventajas de las redes inalámbricas

Como se dijo en el capítulo 2, las principales ventajas que ofrecen las redes inalámbricas frente a las cableadas, son:

- Movilidad
- Desplazamiento
- Flexibilidad
- Ahorro de costes
- Escalabilidad

Expliquemos uno por uno:

- Movilidad:

La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un ordenador o cualquier otro dispositivo pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cale hasta ese sitio.

Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a los recursos compartidos desde cualquier lugar de la red, hacer presentaciones en la sala de reuniones, acceder a archivos, etcétera, sin tener que tener cables por la mitad de la sala o depender de si el cable de red es o no, suficientemente largo.

- Desplazamiento:

Con una computadora portátil o PDA, no sólo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación.

Esto otorga cierto grado de comodidad y facilita el trabajo en determinadas tareas; un ejemplo de esto podría ser la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- Flexibilidad

Las redes inalámbricas no sólo nos permiten estar conectados mientras nos desplazamos con una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red.

En ocasiones, el extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones se termina colocando peligrosos cables sobre el suelo para evitar la molestia de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas.

Las redes inalámbricas resultan especialmente indicadas para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado, existe la necesidad de que varias personas se conecten a la red (en la sala de reuniones, por ejemplo), la conexión inalámbrica evita llenar el suelo de cables.

En sitios donde puede haber invitados que necesiten conexión a Internet (como centros de formación, hoteles, cafés, entornos de negocios o empresariales), las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- Ahorro de costes

Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no sólo económico, sino en tiempo y molestias.

En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación representa problemas; la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos.

- Escalabilidad

Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial.

Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta.

Con las redes cableadas, este movimiento de escalabilidad requiere de la instalación de un nuevo cableado o, lo que es aún peor, esperar que el nuevo cableado quede instalado.

3.6 Desventajas de las redes inalámbricas

Como se observó en el capítulo 2, los principales inconvenientes de las redes inalámbricas son:

- Menor ancho de banda
- Mayor inversión inicial
- Vulnerabilidad a accesos no autorizados.
- Interferencias
- Incertidumbre tecnológica

Expliquemos una por una:

- Menor ancho de banda

Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi Fi lo hacen a 11Mbps.

Ciertamente, existen estándares que alcanzan los 54Mbps y soluciones propietarias que llegan a 100Mbps; sin embargo, estos estándares se encuentran en los comienzos de su comercialización y tiene un precio superior a los de los actuales Wi Fi.

- Mayor inversión inicial

Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos, es superior a los equipos de red cableada.

- Vulnerabilidad a accesos no autorizados.

Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, ya que no se necesita lidiar con los cables; sin embargo, se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.

Como el área de cobertura no está definida por paredes ni por algún medio físico, no es necesario que los posibles intrusos se encuentren dentro del edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan a las redes Wi Fi no es de lo más fiables.

No obstante, también es cierto que las redes inalámbricas ofrecen una seguridad válida para la mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (que recibe el nombre de WPA) que hace a Wi Fi más confiable.

- Interferencias

Las redes inalámbricas funcionan utilizando el medio radio-electrónico en la banda de 2.4 GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada, por lo que muchos equipos del mercado utilizan esta misma banda de frecuencias.

Además, todas las redes WiFi funcionan en la misma banda de frecuencias. Este hecho hace que no se tenga la garantía de un entorno radio-electrónico completamente limpio para que la red inalámbrica funciones a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, mayor será también el rendimiento de la red.

No obstante, el que exista la probabilidad de sufrir interferencias, no lo convierte en un hecho. La mayoría de las redes inalámbricas funcionan perfectamente, sin mayores problemas en este sentido.

3.7 Factores de interferencia en redes inalámbricas

Los factores de atenuación o interferencia de una red inalámbrica son:

a) Tipo de construcción.

b) Micro-ondas.

c) Teléfonos físicos inalámbricos.

d) Dispositivos Bluetooth

e) Elementos metálicos como escaleras de emergencia y armarios.

f) Peceras.

g) Humedad en el ambiente.

h) Tráfico de personas.

- Incertidumbre tecnológica

La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi Fi (IEEE 802.11b).

Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se detenga la actual o, simplemente, se le deje de prestar apoyo.

Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

WI-FI es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11, con este sistema se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varios cientos de metros. Versiones mas recientes de esta tecnología permiten alcanzar los 22, 54 y hasta 100 Mbps.

3.8 Velocidad de las redes inalámbricas

La velocidad máxima de las redes inalámbricas de la tecnología 802.11b es de 11 Mbps; pero la velocidad típica es solamente de la mitad (1.5 Mbps a 5 Mbps) dependiendo de si se transmiten muchos archivos pequeños o unos archivos un poco grandes.

La velocidad máxima de la tecnología 802.11g es de 54 Mbps; pero la velocidad típica de esta última tecnología es solamente unas tres veces más rápida que la de 802.11b (5 Mbps a 15 Mbps).

Si quisiéramos hacer un comparativo entre un tipo de red muy eficiente como es Ethernet con la tecnología inalámbrica, encontraríamos lo siguiente:

Las velocidades típicas de los diferentes tipos de red son:

Con Cables:

- Ethernet 10: (que transmitía a un máximo de 10 Mbps).
- Ethernet 10/100: (sucesora de ethernet 10) que transmite un máximo de 100 Mbps y tiene una velocidad típica de entre 20 y 50 Mbps. Compatible Con Ethernet 10.
- Ethernet 10/100/1000: Es la más usada ahora en tecnología con cables y 10 veces más rápida que la anterior. Como se ha empezado a instalar a la par que las redes inalámbricas tiene que luchar con la versatilidad y facilidad de implantación de éstas. Compatible con las dos anteriores.

Sin Cables:

- 802.11b: Aproximadamente entre 1.5 y 5 Mbps
- 802.11g: Aproximadamente entre 5 y 15 Mbps. Compatible con la anterior.
- 802.11n: Estándar compatible con las anteriores.

3.9 Transmisión de la información en redes inalámbricas

La información en redes inalámbricas se transmite por radio frecuencia (RF) a través del aire. La información se envía en paquetes.

Hay tres tipos diferentes de paquetes:

- Paquetes de Manejo (Management)
- Paquetes de control
- Paquetes de datos

Los paquetes de manejo establecen y mantienen la comunicación. Los paquetes de control ayudan a la entrega de datos. Los paquetes de datos contienen las direcciones del remitente y del destinatario, entre otras cosas.

Estos paquetes en los que se envía la información, se subdividen en otros de acuerdo con el tipo de información que manejan. En la figura 3.8 se observa un cuadro sinóptico que muestra esta subdivisión:

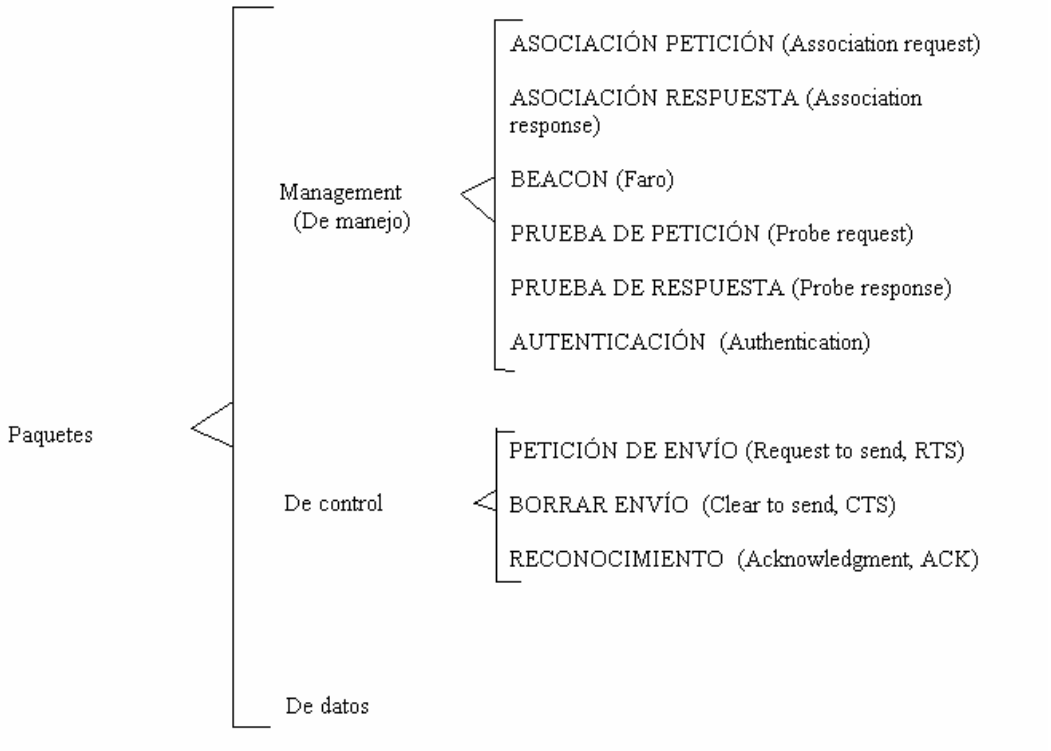


Figura 3.8 Subclasificación de paquetes en tecnología inalámbrica

Las subdivisiones marcadas, no serán vistas en este trabajo, a razón de no expandirse demasiado en este tema.

La velocidad de transmisión de una red inalámbrica Wi Fi será en fundón de la distancia, los obstáculos y las interferencias.

3.10 Número de usuarios

La cantidad óptima de usuarios que pueden conectarse a un punto de acceso va en función del ancho de banda requerido. A medida que se conectan más usuarios, se va repartiendo el ancho de banda entre todos, disminuyéndolo. Y si el ancho de banda se disminuye demasiado, la conexión será de muy baja calidad.

Para realizar la estimación de la cantidad de puntos de acceso que necesitará una red inalámbrica, es necesario conocer antes, el perfil de los usuarios y el tipo de aplicaciones que utilizan; puesto que el consumo de ancho de banda varía entre cada aplicación.

Una vez establecido el ancho de banda que necesita cada grupo de usuarios, hay que analizar el porcentaje de uso de la red (tomando en cuenta que se realizan otras actividades que no necesitan la red).

La fórmula para calcular la cantidad de puntos de acceso necesarios es:

$$\text{NÚMERO DE PUNTOS DE ACCESO} = \frac{\text{ANCHO DE BANDA} * \text{NÚMERO DE USUARIOS} * \text{\% DE UTILIZACIÓN}}{\text{VELOCIDAD PROGRAMADA}}$$

Por ejemplo, si una red tiene cien usuarios y desea, para cada usuario, un ancho de banda de 1 Mbps; el uso de la red no es muy exigente y abarca solamente el 25% y la velocidad estimada es de 5.5 Mbps, tendríamos:

$$\text{4.5 puntos de acceso} = \frac{1 \text{ Mbps} * 100 \text{ usuarios} * 0.25}{5.5 \text{ Mbps}}$$

Como no se pueden colocar fracciones de punto de acceso, se eleva al siguiente entero; en este caso, se requiere de cinco puntos de acceso.

En aquellos casos en los que no se dispone de alguno de los datos anteriores, se puede utilizar, como primera aproximación, la cantidad de ocho a diez usuarios por punto de acceso.

3.11 Amenazas a solucionar en redes inalámbricas

Las redes inalámbricas tienen ciertas características que las hacen vulnerables, lo que determina una gran desventaja y un problema que, actualmente, puede solucionarse (por lo menos en parte).

Hablando de redes inalámbricas, se sabe que todos los que estén en un radio de 100 metros, aproximadamente, son intrusos potenciales. La información se transmite por el aire y, por lo tanto, puede ser vista por cualquiera dentro de este margen.

Los usuarios pueden conectarse equivocadamente (o voluntariamente) a redes que se encuentren abiertas en el radio mencionado; lo cual supone un peligro para cualquier organización, puesto que un “intruso” puede captar los login y contraseñas cuando los usuarios intenten conectarse.

Por ello, se han incluido en redes Wi Fi ciertos mecanismos de seguridad que permiten encriptar la comunicación entre los diversos elementos de una red inalámbrica Wi Fi.

El primero de estos mecanismos fue el WEP (Privacidad equivalente a una red cableada o Wired Equivalent Privacy); sin embargo, este sistema tiene algunas debilidades.

WPA (Wi Fi Protected Access o acceso protegido Wi Fi) y WPA2 son dos protocolos de encriptación que se desarrollaron para solucionar las debilidades detectadas en el WEP.

Existen dos versiones de WPA:

- Una “home” o personal, que es para uso casero y de pymes; y
- Una más robusta denominada “Enterprise”.

3.12 Gestión de red inalámbrica

La gestión de una red inalámbrica es un proceso permanente y continuo, las 24 horas del día.

Las funciones y tareas requeridas para la gestión y control de una red Wi Fi son:

- Instalación y configuración.
- Administración.
- Problemas de conexión y mantenimiento.
- Control de rendimiento.
- Gestión de la seguridad.

En la figura 3.9 se observa el ciclo para la gestión de una red inalámbrica Wi Fi:

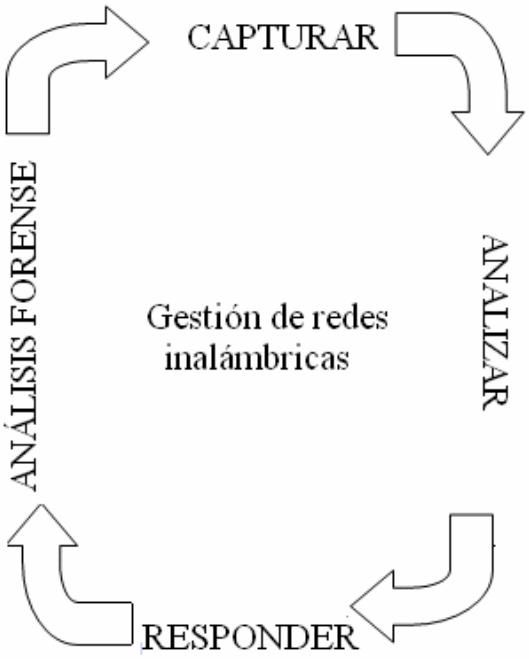


Figura 3.9 Ciclo de gestión de una red inalámbrica

3.13 Visión a futuro

Las aplicaciones de las redes inalámbricas son infinitas (prácticamente). Por el momento, crean una nueva forma de usar la información; esto debido a que estará al alcance de todos a través de Internet, y en cualquier lugar (en el que haya cobertura).

Se cree que en un futuro cercano, se reunificarán todos los dispositivos con los que hoy contamos, para dar paso a la nueva evolución: Nuevos dispositivos en las cuales estarán reunidas las funciones de comunicación, sin tener que dispersarlos en varios elementos (su nombre podría ser: Terminales Internet).

También podría tener cabida a una Internet paralela y gratuita, que estaría basada en redes altruistas, las cuales funcionarían de acuerdo a lo que cada uno de los usuarios pusiera a disposición en la red, y en donde las personas puedan incorporarse a este tipo de red.

En un futuro, la conjugación de las redes Mesh con las redes inalámbricas y las redes Grid, podría llevar a cabo el nacimiento de nuevas formas de computación que permitan cálculos inimaginables hasta ahora debido a los requerimientos de hardware.

La tecnología para llevar a cabo esto, existe desde hace tiempo; su precio es accesible y su existencia depende de las estrategias comerciales de las empresas que las poseen.

CAPÍTULO 4:

ESTRATEGIA Y METODOLOGÍA DE DISEÑO

CAPITULO 4:

ESTRATEGIA Y METODOLOGÍA DE DISEÑO

4.1 Antecedentes

Las redes informáticas y su constante evolución han permitido el avance en la difusión de la información a nivel mundial.

Día a día, se ve como los sistemas de redes evolucionan, volviéndose cada vez más eficientes, pero también más complejos en su diseño e implantación.

Partimos del hecho de que las redes informáticas tienen notorios cambios entre ellas; razón por la cual se deben conocer sus características si se desean armar "correctamente".

Hacemos mención de algunos puntos importantes que atañen a este tema:

- El diseño de una red inalámbrica Wi Fi, requiere de amplios conocimientos sobre la tecnología mencionada; sobre las diferentes arquitecturas de redes inalámbricas; y nociones avanzadas correspondientes a la seguridad Wi Fi.

- Los parámetros que deben controlarse en una red Wi Fi son muy diferentes que en las redes cableadas.

- Los conocimientos que poseen muchos profesionales informáticos sobre las redes cableadas (redes tradicionales), no son suficientes para lograr un diseño óptimo de una red inalámbrica. Sabemos que no todas las personas (aún teniendo conocimientos informáticos) son capaces de crear eficientemente una red inalámbrica, puesto que esta tiene necesidades especiales y muchos factores que tomar en cuenta para hacerla eficiente y lo más segura posible.

- En una red cableada existen básicamente tres variables a manejar; mientras que en una red inalámbrica Wi Fi son más de diez variables y es muy difícil estar adivinando las soluciones.

4.2 Errores comunes en el diseño

La mayoría de las redes inalámbricas Wi Fi que existen, están mal diseñadas (si es que fueron diseñadas; puesto que muchas redes inalámbricas están hechas sin un diseño profesional previo y se han ido construyendo de acuerdo a las fallas que se van presentando; agregando parches para "solucionar" los problemas) y con muy escasa conciencia en cuanto a seguridad Wi Fi se refiere.

Los problemas en redes inalámbricas radican en el apoyo del usuario en las personas equivocadas y/o en el poco interés en poner escuchar (y practicar, por supuesto) consejos y recomendaciones de expertos en la materia.

Los errores más comunes que se cometen al querer diseñar y/o implantar una red inalámbrica, se podrían enumerar como sigue:

- Hacer caso a los consejos que dan los vendedores de hardware, sin tomar conciencia de que su trabajo es el de vender y no el de buscar la satisfacción de las necesidades del cliente. En este supuesto, el cliente termina comprando dispositivos que no va a ocupar o que finalmente tendrá que desechar porque le causa muchos problemas en la red. La forma de resolver este problema es buscar suficiente información al respecto de las redes inalámbricas y buscar ayuda de un profesional en la materia.

- Mezclar marcas y tecnologías diferentes. Este caso es muy común y supone un grave problema en el sentido de compatibilidad; si bien es cierto que estos dispositivos pueden trabajar juntos, tienen que eliminar, cada uno, algunas funciones para poder ser utilizados; lo que implica una baja calidad y eficiencia de la red. Lo mejor, si no conocemos las características y compatibilidades de los equipos, es obtener equipo de la misma marca y tecnología.

- No realizar un estudio previo de acuerdo a las necesidades y los requerimientos. Generalmente, se da por hecho que las redes inalámbricas funcionan (o deben funcionar) exactamente como las cableadas; hecho que no es verdad. Cuando no se realiza este estudio, se corre el riesgo de que, en un periodo no muy grande de tiempo (unos seis meses) se tenga que reconstruir la red, al presentar un sin número de problemas.

- Planear y diseñar una red pensando solamente en el momento actual, y no tomar en cuenta las cambiantes necesidades en el futuro. Esto provoca que, a través del tiempo, la red se vuelva obsoleta y sin la más remota posibilidad de actualizarse. Sabemos que las redes inalámbricas Wi Fi son escalables, esto es, se pueden actualizar de acuerdo a las cambiantes necesidades de los usuarios; para que esto sea posible (por supuesto), es necesario diseñar la red de manera que tome en cuenta que, en el futuro, deberá adaptarse a los requerimientos del momento.

- "Olvidar" de poner reglas de uso de la red inalámbrica. La falta de políticas documentadas de uso, cada usuario podrá resolver los problemas que se presenten, según su "buen juicio", convirtiendo la red en un literal desastre. Las políticas en una organización son muy importantes y el respetarlas sumamente importante, este respeto debe darse en todos los niveles de la organización.

- No capacitar a los usuarios ni a los ejecutivos sobre el uso de la tecnología inalámbrica. El mal conocimiento del uso y manejo de redes supone un gran problema a corto plazo; generalmente, los más afectados son los miembros de la organización y la culpa se la echan encima al diseñador de la red. La eficiencia de una red (incluso las cableadas) depende, en gran medida, del tipo de uso que se le dé y del conocimiento que los usuarios tengan respecto de su manejo; la mejor red puede ser detrimentada en su eficiencia por el mal manejo.

- No preparar instrucciones para configurar los puntos de acceso. Cuando en una red inalámbrica existen más de un puntos de acceso, es importante que todos estén configurados de la misma manera; sin embargo, como cada punto de acceso, usualmente, es configurado por una persona diferente, quedan configurados sin tomar en cuenta a los otros. Esto crea espacios de incompatibilidad y puede crear deficiencia en el sistema de comunicaciones si no se encuentran las instrucciones "estándar" más adecuadas por escrito.

- Administrar la red de manera descentralizada. Cuando una red tiene dos o más administradores, la gestión se convierte en una amenaza en cuanto a que cada administrador define las funciones, usuarios y tareas de manera diferente, y puede dar lugar a una colisión. Por otro lado, si se mantiene centralizadamente el uso de la red inalámbrica, un solo administrador tendrá la tarea de asignar claves y dar acceso sólo a usuarios y aplicaciones particulares.

- No monitorear la red ni su seguridad. Las redes inalámbricas funcionan de manera diferente a las redes cableadas y, constantemente presentan desafíos en materia de seguridad; hay que tomar muy en cuenta los factores que pueden provocar algún tipo de interferencia (dispositivos de radiofrecuencia, construcciones, medio ambiente); tampoco se puede esperar que una red inalámbrica funcione igual en todos los lugares, puesto que las condiciones del medio ambiente cambian. Lo recomendable en este caso es realizar pruebas a diferentes horas y colocando los ordenadores en diferentes lugares (del mismo inmueble) para revisar el nivel de interferencia de cada zona.

- No encriptar la información. Cuando se habla por medio de una red inalámbrica, de manera muy clara, se corre el riesgo de que cualquier persona pueda acceder a la información que tenemos y, si ésta es importante, se crean grandes riesgos. En ocasiones, se encripta utilizando WEP, que es el protocolo más antiguo y, como vimos en el capitulo 3, tiene grandes huecos. Por supuesto, es más fácil sólo plantarlo sin preocuparse demasiado por la seguridad. Aquí, es conveniente hacer notar la importancia de los protocolos WAP y WAP2, cuya construcción se realizó precisamente para incrementar la seguridad en las redes wireless y llenar los huecos del anterior protocolo WEP.

- No cambiar las claves iniciales de los dispositivos. Cuando los dispositivos simplemente son instalados y no se le cambian claves ni atributos, es muy sencillo que se realicen accesos “no autorizados”. Es recomendable que, al instalar los dispositivos (como puntos de acceso, por ejemplo) le sean cambiados los códigos que traen por defecto por unos personalizados; la finalidad es que el acceso a la red inalámbrica se restrinja lo más posible.

- No preocuparse por si es sencillo o no realizar conexiones desde el exterior (puntos de acceso hostiles). Pueden ser originados por empleados mal intencionados o negligentes, por hackers y por vecinos (accidental o intencional). Este tipo de conexiones, cuando existen, pueden causar graves daños a la seguridad de la organización, puesto que rompen la seguridad perimetral; si este análisis no se realiza, incluso se corre el riesgo de que entren virus informáticos a nuestro sistema de ordenadores, así como ataques de hackers, etcétera.

- Asegurarse de que los usuarios no conozcan los peligros en Hotspots, aeropuertos, hoteles y aviones y que no conozcan las redes Ad-hoc. Los puntos de caceso públicos, denominados Hotspots, se están difundiendo a un ritmo veritiginoso y presentan numerosos riesgos a los usuarios. Esto se agrava si los usuarios desconocen los riesgos. Cuando una computadora portátil se activa en un lugar público, la vecindad (alrededor de 100 mts.) se abre a cualquier usuario que desee acceder a la red; lo que puede llevar al robo de claves e información.

- Ahorrarse el servidor RADIUS y no autenticar a los usuarios según el estándar IEEE 802.1x. Este es uno de los errores más grandes que cometen muchas empresas: No utilizar servidores RADIUS para autenticar y autorizar. El diseño de una red inalámbrica wifi robusta y con una seguridad informática profesional, requiere conocimientos y capacitación. No es sencillo y no es en nada similar a las redes cableadas. Elementos como el servidor RADIUS y los protocolos EAP, son características exclusivas de las redes wifi. Es una tecnología nueva y es normal que muchos la desconozcan. Entonces, también es normal que para asegurar buenos resultados se deba consultar a expertos asesores que ya tengan experiencia en este tipo de instalaciones.

- Invitar a usuarios, proveedores y cliente a traer sus propios equipos y conectarlos a la red Wi Fi de la organización. En la actualidad, son muchas las empresas e instituciones que "facilitan" a los visitantes como proveedores, auditores, clientes, etc. la utilización de recursos y la conexión a la red empresarial. Estos computadores, suelen ser la causa de muchas infecciones de virus de PC y/o pérdidas de información "inexplicables". Cabe mencionar que diversas empresas practican esta actividad y, si esto es necesario para una organización, todos los accesos deben ser regulados y verificados por el administrador, previa autorización de los ejecutivos de la organización.

4.3 Diseño de una red inalámbrica

La mayoría de las redes inalámbricas que hay en el mercado funcionan de una manera muy similar; tienen unas estaciones de base o puntos de acceso, que coordinan las comunicaciones; y unas tarjetas de red o adaptadores de red, que se instalan en los equipos y que les permiten formar parte de la red.

Asimismo, existen antenas que permiten el aumento en el alcance de los equipos Wi-Fi, así como software especializado que facilita la labor de gestión y mantenimiento de la red inalámbrica.

Antes de describir los distintos componentes requeridos para crear una red Wi-Fi, se hace necesario describir las características más importantes para una selección adecuada de algún tipo de arquitectura Wi-Fi, así como los parámetros a considerar para su implementación.

4.4 Consideraciones para el diseño

Para el diseño de una red, se deben de tomar en cuenta varios factores, los cuales serán característicos del tipo de aplicación de la red.

Los aspectos a tomar en cuenta son:

- Lugar de instalación
- Número de servidores
- Número de terminales
- Dispositivos de interconexión
- Medios de transmisión
- Tarjetas de red
- Software
- Estándares

4.5 Dispositivos inalámbricos

Sea cual sea el estándar que se elija, se dispone principalmente de dos tipos de dispositivos:

- Dispositivos “Tarjetas de red” o TR.
- Dispositivos “Puntos de acceso” o PA.

Los dispositivos "Tarjetas de red", o TR serán los que tengamos integrados en nuestro ordenador; o bien, conectados mediante un conector PCMCIA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa.

Estos dispositivos sustituyen a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados en las redes cableadas. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Los dispositivos "Puntos de Acceso", ó PA serán los encargados de recibir la información de los diferentes TR de los que conste la red; para su centralización o para su encaminamiento. Complementan a los Hubs, Switches o Routers.

Si bien los Puntos de Acceso pueden sustituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

Recordando la visión de una red inalámbrica, se observa la figura 4.1

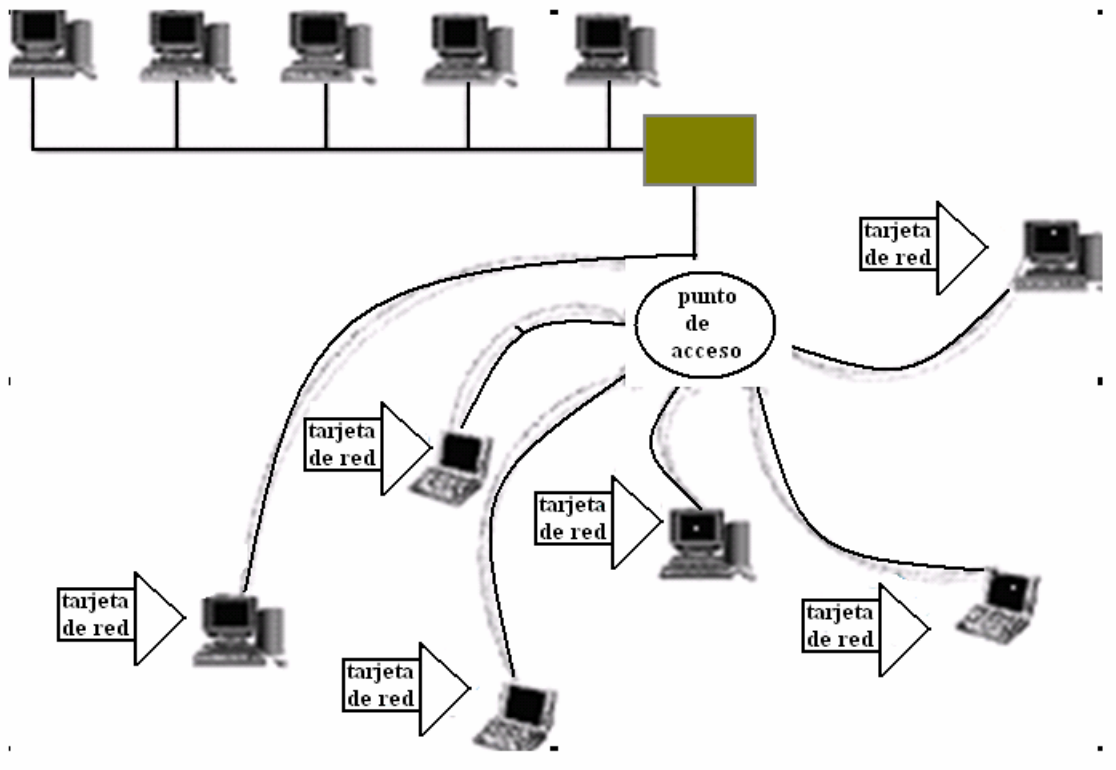


Figura 4.1 Representación gráfica de una red inalámbrica

4.6 Funcionamiento de los dispositivos

Todos los estándares aseguran su funcionamiento mediante la utilización de dos factores:

- Cuando estamos conectados a una red mediante un cable, sea del tipo que sea, disponemos de una velocidad fija y constante.
- Cuando estamos hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores.

Cuando una tarjeta de red se conecta a un punto de acceso, se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del Punto de Acceso (normalmente en 802.11g será de 54Mbps)
- Distancia al PA (a mayor distancia menor velocidad)

- Elementos intermedios entre la Tarjeta de Red y el Punto de acceso (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el Punto de Acceso y la Tarjeta de Red modifican la velocidad de transmisión a la baja).

- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias).

Normalmente los fabricantes de Puntos de Acceso presentan un alcance teórico de los mismos que suele andar alrededor de los 300 metros. Esto obviamente es sólo alcanzable en condiciones de laboratorio, pues realmente en condiciones objetivas el rango de alcance de una conexión varía (y siempre a menos) por la infinidad de condiciones que le afectan.

Cuando ponemos una Tarjeta de red cerca de un Punto de acceso, disponemos de la velocidad máxima teórica del Punto de acceso (54 Mbps, por ejemplo), y conforme nos vamos alejando del Punto de acceso, tanto él mismo como la Tarjeta de red, van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia.

Así, se podría decir que en condiciones "de laboratorio" y a modo de ejemplo teórico, la transmisión entre dispositivos 802.11 podría ser como se muestra en la figura 4.2:

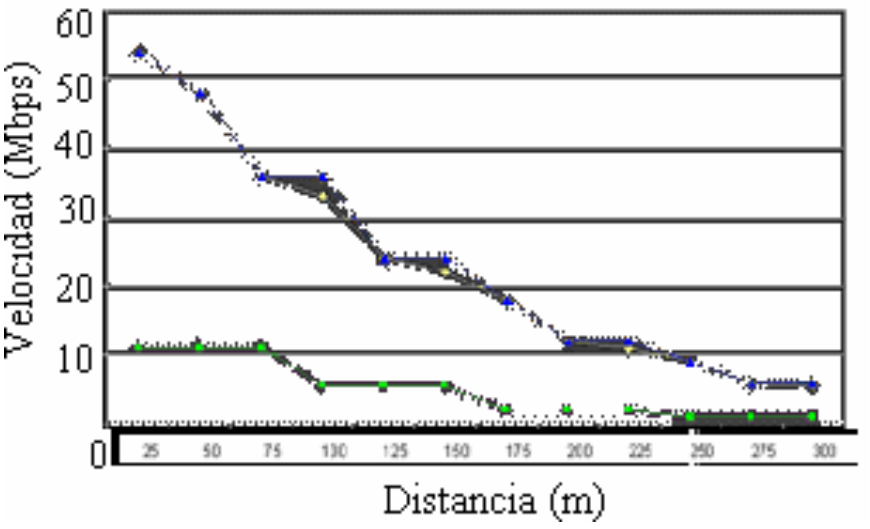


Figura 4.2 Transmisión de información en valores de laboratorio

4.7 Antenas

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX (transmisión y recepción) de los dispositivos wireless (inalámbricos).

Dentro de los Puntos de acceso (actualmente ya se puede comenzar a aplicar también a las Tarjetas de red), se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en:

- Direccionales
- Omnidireccionales.

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

Cabe mencionar que muchos particulares se han construido sus propias "antenas caseras" con diferentes resultados

4.8 Transmisión de la información

Cuando se transmite información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits.

Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, como son:

- Barker. (RTS / CTS)
- ?- CCK. Complementary Code Keying
- ?- PBCC. Packet Binary Convolutional Coding
- ?- OFDM. Orthogonal Frequency-Division Multiplexing

La figura 4.3 muestra una representación gráfica de las tramas más importantes:

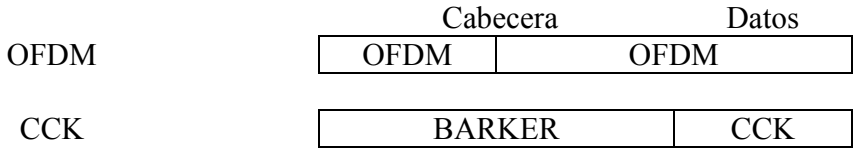


Figura 4.3 Tramas más importantes

Se puede observar en la figura, que la cabecera, en el caso de la codificación OFDM es más pequeña. A menor tamaño de cabecera menor "overhead" en la transmisión; es decir, menor tráfico de bits de gestión luego mayor "sitio" para mandar bits de datos. Lo que repercutirá positivamente en el rendimiento de la red.

Ya a primera vista podemos ver que el estándar 802.11g es una unión de los estándares 802.11 "a" y "b". Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, mientras que los otros dos operan en la del los 2.4 Ghz.

Cuando se tiene una red inalámbrica en la que todos los dispositivos son tipo "a" o todos de tipo "b" no hay problemas en las comunicaciones. Cada Punto de acceso tipo "a", tendrá sólo Tarjeta de red tipo "a" y los Puntos de acceso tipo "b", tendrán sólo Tarjetas de red tipo "b". Se selecciona la mejor modulación y se transmite.

Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible.

En el caso de dispositivos AP 802.11g normalmente estaremos usando la modulación OFDM, modulación que es la óptima para este estándar.

Si por un casual un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b", cosa que es capaz de hacer. Sin embargo, el dispositivo "b" no puede escuchar las transmisiones de los otros dipositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender.

Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, no por que interfieran ya que usan diferente modulación sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos "b" usan la modulación Barker con TRS/CTS (Request To Send / Clear To Send), que básicamente significa que deben pedir permiso al AP para transmitir.

En este momento, es conveniente diferenciar entre las topologías y el modo de funcionamiento de los dispositivos Wi Fi:

Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

Como se vio en el capítulo 3, en el mundo inalámbrico existen dos tipos de topología básicas: Ad-hoc e Infraestructura.

Un caso especial de topología de redes inalámbricas es el caso de las redes Mesh.

Todos los dispositivos, independientemente de que sean Tarjetas de red o Puntos de acceso, tienen dos modos de funcionamiento:

- Modo Managed, es el modo en el que el TR se conecta al AP para que éste último le sirva de "concentrador". El TR sólo se comunica con el AP.

- Modo Master. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento sugieren que, básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como Puntos de acceso realmente Tarjetas de red a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW.

Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP - OPENAP.

Esta afirmación se ve confirmada al descubrir que muchos Puntos de acceso, en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como TR.

4.9 Seguridad en redes inalámbricas

La seguridad es una de los temas más importantes cuando se habla de las redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

4.9.1 Terminología

Para poder entender la forma de implementar mejor la seguridad en una red wireless, es necesario comprender primero ciertos elementos:

- WEP. Significa Wired Equivalet Privacy, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

- OSA vs SKA. OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el Punto de acceso. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo Tarjeta de red pide al Punto de acceso autenticarse. El Punto de acceso le envía una trama a la Tarjeta de red, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

- ACL. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

- CNAC. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

- SSID. Significa Service Set IDentifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Las Tarjetas de red deben conocer el nombre de la red para poder unirse a ella.

4.9.2 Pasos para asegurar una red inalámbrica

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático.
Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener. Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red wireless.

Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar "desperdigando" la información hacia los cuatro vientos con todo lo que esto conlleva.

De esta forma, los pasos necesarios para asegurar una red wireless serían:

- **Paso 1**, debemos activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

- **Paso 2**, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por oes...

- **Paso 3**, uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

- **Paso 4**, desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

- **Paso 5**, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial reconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

- **Paso 6**, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

- **Paso 7**, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente, el IEEE está trabajando en la definición de nuevos estándares 802.11 que permitan disponer de sistemas de comunicación entre dispositivos wireless realmente seguros.

También hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

4.10 Red inalámbrica de uso personal

Una red inalámbrica de uso personal es, actualmente, uno de los escenarios más comunes de esta tecnología.

Hasta hace bien poco los usuarios "caseros" de ordenadores, bien por uso particular bien por uso profesional del ordenador y por ende de Internet, estaban "atados" a las zonas de la casa/local donde tenían las tomas telefónicas o bien los módems ADSL/DSL/CABLE. El mover los ordenadores a otra localización dentro de la casa / pequeño negocio era prácticamente imposible o muy costoso.

Además, con el continuo avance de la tecnología y el rápido desfase de los ordenadores nos podemos encontrar en una casa normal con varios ordenadores unidos mediante una LAN (red de área local) y eso significaba que tanto el módem como los ordenadores debían estar en un espacio muy reducido, normalmente poco idóneo para su uso y/o ubicación.

Este hecho, unido con la "habilidad" de ciertos constructores que se han dedicado a poner las toma telefónicas y/o las tomas de ADSL/DSL/CABLE en los lugares más originales pero menos aprovechables de las casas podía llegar a presentar un serio inconveniente para implantar una pequeña red.

Gracias a la tecnología inalámbrica actual, es posible solucionar este problema de una manera muy fácil y nos va a permitir disponer de los ordenadores en la situación que queramos dentro de la casa.

4.11 Implantación de red de uso personal

Supongamos que tenemos una casa con tres computadoras: dos de ellos de sobremesa y uno portátil. Esta configuración es una configuración estándar que representa bastante bien un amplio espectro de los hogares medios, en los cuales uno de los ordenadores se ha quedado tecnológicamente desfasado pero aún se quiere aprovechar. Se ha comprado un segundo ordenador de sobremesa más potente y se tiene uno portátil bien por necesidades particulares o bien porque el trabajo de uno de los integrantes de la familia lo provee.

Suponemos que disponemos bien de una conexión telefónica o bien un ADSL/DSL/CABLE para conectarnos a Internet.

La lista de elementos que vamos a necesitar para implantar la red es muy corta:

- Ordenador 1 (ya disponible)
- Ordenador 2 (ya disponible)
- Ordenador portátil (ya disponible)
- 1 tarjeta PCI WiFi 802.11b (a adquirir)
- 1 tarjeta USB WiFi 802.11b (a adquirir)
- 1 tarjeta PCMCIA WiFi 802.11b (a adquirir)
- 1 PA Router Wifi 802.11b (a adquirir)

La configuración más normal será la de configurar el ordenador más tecnológicamente atrasado con la tarjeta Wifi PCI, poniendo la USB WiFi al ordenador más moderno y dejando la PCMCIA WiFi para el ordenador portátil.

Lo preferible sería ponerle a los dos ordenadores de sobremesa TR USB WiFi, pero si no disponemos de puerto USB o no tenemos ninguno libre en el ordenador antiguo habrá que ponerle tarjeta PCI WiFi.

Cabe mencionar que, en el caso de conectar tarjetas USB WiFi, debemos tener en cuenta que el USB 1.1 sólo permite transferir datos a una velocidad máxima de 12 Mbps por lo que si le conectamos una tarjeta USB WiFi 802.11g con una velocidad máxima de 54 Mbps no conseguiremos aumentar la velocidad. Para conectar este tipo de tarjetas es necesario disponer de conectores USB 2.0.

El Punto de acceso Router será el encargado de conectarnos a Internet. Hay algunas unidades que llevan un MODEM 56K V90 integrado por lo que no es necesario comprar un MODEM adicional.

En cualquier caso usar un MODEM para conectarse a Internet debería de ser la última de nuestras opciones, pues es muy recomendable el contratar las ya baratas soluciones ADSL / DSL / CABLE de cualquier proveedor que nos la ofrezca.

Es caso del ADSL, por ejemplo y del DSL y CABLE por extensión, los routers disponen de una entrada WAN a la cual enchufar el MODEM sea del tipo que sea, por lo que el configurarlo será muy sencillo. Para este caso, supongamos una salida a internet mediante ADSL 256/128 Kbps.

Es muy interesante que disponga de Servicio DHCP (asignación dinámica de direcciones IP) y de NAT (traducción/asignación de direcciones IP mediante el uso de direcciones privadas del tipo 198.162.x.x ó 10.x.x.x) lo que nos permitirá permanecer protegidos de las "inclemencias" de internet.

El Punto de acceso Router distribuirá la señal entre los tres ordenadores, que ahora podremos poner en cualquier sitio. La configuración normal será que el niño / joven de la casa disponga del más potente para jugar en su habitación, el / los padres del tecnológicamente desfasado pero seguro para almacenar su documentación y navegar por internet en su despacho y el ordenador portátil se reservaría para hacer en casa (sigh!!) cosas del trabajo y poco más.

Dado que tenemos tres adaptadores "recibiendo" información desde internet, y dada la conexión ADSL con 256 Kbps de bajada, en el peor momento punta tendremos

256 Kbps/3 = 85.32 Kbps para cada uno,

el cual parece un ancho de banda razonable, es más, dadas las características de los tres aparatos es altamente improbable que los tres estén conectados al mismo tiempo, y en ese caso de los tres conectados, es poco probable que estén los tres recibiendo información al máximo de su velocidad al mismo tiempo.

En la figura 4.4, podemos observar esto de manera gráfica:

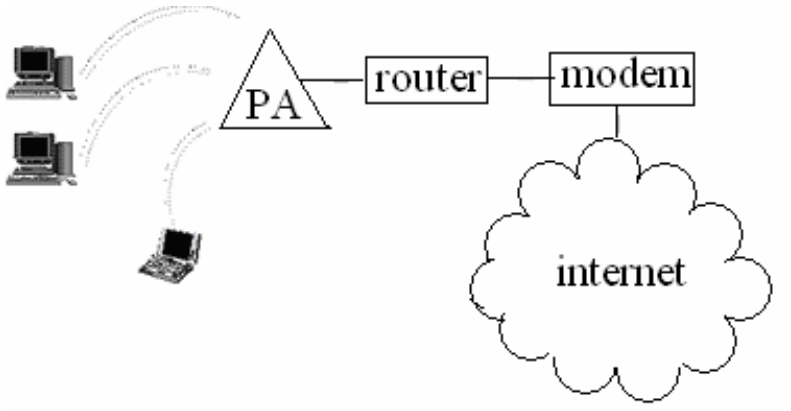


Figura 4.4 Red personal con tres ordenadores

Para realizar este tipo de red es deseable usar un tipo de conexión 802.11b que nos va a permitir conectarnos a Internet sin ningún problema además de transferir archivos entre las máquinas y compartir recursos sin ningún problema de velocidad.

La configuración recomendada es la de más alta seguridad, tal y como se ha detallado en el apartado correspondiente a seguridad. El único paso que podemos obviar sería el uso de redes VPNs, aunque de todas formas sea recomendable su uso.

Tomando como ejemplo de marca a seleccionar a D-link, los precios (sin IVA) pueden ser los que siguen (sólo válidos como guía para este estudio):

- D-Link DWL-520+ PCI 61.12 US Dollar
- D-Link DWL-650+ PCMCIA 50.00 US Dollar
- D-Link DWL-120 USB 60.43 US Dollar
- D-Link DWL-900AP+ AP 122.22 US Dollar

Lo cual hace un total de 293.34 US Dollar, cantidad perfectamente asumible por una familia media o pequeño negocio.

Si lo comparamos con el equivalente necesario (sin contar con el tiempo para realizar la instalación y los conocimientos que son necesarios) para instalar una red Ethernet típica a 10/100 Mbps, podemos llegar a la conclusión de que la red inalámbrica:

- Es más barata
- Es más fácil de configurar
- Nos permite conectar los ordenadores independientemente del lugar en donde se hayan colocado los ordenadores.
- Evita la instalación de incómodas canaletas por el suelo y las paredes.

4.12 Estándares?

Los estándares son tan buenos que cada fabricante tiene el suyo. Esto, que parece ser una broma, que no puede ser más cierta en el caso que nos incumbe.

La proliferación de diferentes estándares viene dada únicamente por la prisa que tienen algunas compañías en introducirse en los mercados emergentes para alcanzar una posición de fuerza y poder manejar de la forma que sea más beneficioso para sus intereses las decisiones de los comités estandarizadores del IEEE.

Idealmente, todas las empresas deberían seguir los estándares del IEEE para asegurar la interoperabilidad de los dispositivos vendidos con los dispositivos de otros fabricantes, pero lamentablemente eso no ocurre así y diferentes fabricantes ofrecen diferentes soluciones que terminan por no funcionar entre sí.

Esta situación se vivió en los principios de la venta masiva de dispositivos SCSI en los que era mejor adquirir todos los dispositivos SCSI de un mismo fabricante pues si por un lado adquiríamos la tarjeta y por otro los dispositivos podíamos tener incompatibilidades que nos obligaban a tener que tirar uno de ellos a la basura. Bueno pues esa misma situación es en la que nos encontramos hoy en día.

Aunque muchos fabricantes prometen en sus folletos de venta que sus dispositivos no estandarizados cumplirán con las especificaciones del IEEE cuando éste publique el estándar correspondiente, bien sin modificaciones bien mediante una actualización de su Firmware, esto es algo de lo que no podemos estar totalmente seguros.

4.13 Metodología

Tal vez los puntos anteriores no hayan sido suficientemente claro para la implantación de una red inalámbrica en casa; así que vayamos de la mano paso por paso:

4.13.1 Necesidades para montar una red de uso personal en casa

La mejor configuración es partir de una conexión ADSL con router, aunque también podremos montar una red Wi-Fi en casa a partir de otras configuraciones (cable, etc.). Si ya contamos con esto, necesitaremos además:

- Punto de Acceso Wi-Fi.
- Si nuestro ordenador o portatil no incluye WiFi, necesitaremos un accesorio que nos de este tipo de conectividad.

4.13.2 Configuración del Access Point

Hay que aclarar que existen en el mercado decenas de marcas y cientos de modelos de puntos de acceso.

Antes de comprar un punto de acceso inalámbrico, es recomendable verificar sus características en la página web de la Wi Fi Alliance.

Es importante evaluar seriamente si está previsto utilizar funciones complejas o es mejor economizar. Aunque un punto de acceso robusto ofrece las funciones de: firewall, utilizades para el Site Survey de redes inalámbricas y otras más, se debe prever si se van a usar; si no es así, es mejor optar por un punto de acceso básico.

En la forma más general, los pasos a seguir serían:

1) Sacar el Punto de acceso de su caja y conectarlo a la red eléctrica con el alimentador incluido en la caja.

2) Conectar el Punto de acceso al router ADSL con el cable cable de red del AP (también incluido en la caja).

3) Si se tiene DHCP activado en el router ADSL en principio no habrá que configurar ningún parámetro adicional en el AP.

Si el DHCP está activado, el router asigna automáticamente una dirección IP al equipo que se está conectando, sin necesidad de especificar algunos datos en la configuración de red del equipo (IP, puerta enlace, etc.). Todos estos datos los proporciona el router de forma automática.

Si no se tiene DHCP activado, se tendrá que establecer en el Punto de acceso la IP privada que tendrá, la puerta de enlace (IP del router), la máscara de subred y los servidores DNS.

En todos los Puntos de Acceso se puede entrar al panel de administración a través de un navegador web. Algunos incluyen además un programa de Windows para hacer esta configuración. En cualquier caso consultar el manual del AP para información detallada.

4.13.3 Configuración del equipo

Para conectar un ordenador portátil o de sobremesa, consulta el manual de usuario para información detallada de la configuración.

Lo más normal es que tenga una herramienta de gestión de la conexión Wi-Fi, incluida con el accesorio, donde se podrán configurar los parámetros necesarios, así como ver la potencia de la señal.

Si se tiene DHCP activado sólo se tendrá que abrir este programa, escanear las redes disponibles, seleccionar la nuestra y conectaros a ella. La configuración se realizará automáticamente.

Si se tiene DHCP desactivado se tendrá que establecer manualmente la dirección IP del equipo, la puerta de enlace, la máscara de subred y los servidores DNSs. Después de hacer esto abrir el programa de configuración de Wi-Fi del equipo o del accesorio que se haya instalado y seguír los pasos del párrafo anterior.

4.13.4 Consideraciones y consejos sobre alcance y cobertura

Al instalar una red inalámbrica Wi Fi hay que tener muy en claro el objetivo del proyecto.

Hay quienes lo hacen por estar a la moda; en otros casos se busca favorecer la “movilidad” de los usuarios; o se hace por estética (para no ver cables); o por costos; puesto que en la actualidad, una red inalámbrica Wi Fi puede ser más económica que una red cableada.

Independientemente de cual sea la motivación, siempre habrá una condición primordial que cumplir: Hay que lograr una buena productividad de los usuarios y que la calidad del servicio no sea muy inferior a la de las redes cableadas.

Esta condición nos enfrenta a un primer inconveniente: Los usuarios de un punto de acceso deben compartir el ancho de banda. Es decir, mientras más usuarios estén conectados a un punto de acceso inalámbrico, menos ancho de banda habrá para cada uno de ellos.

Por lo tanto, debemos evitar cometer un error muy común de los principiantes, que desconocen el funcionamiento de las redes inalámbricas Wi Fi: Buscar sólo cobertura y descuidar la capacidad.

Muchos se preocupan, al principio, por el alcance o cobertura de la red Wi Fi. En las redes empresariales este no es un punto tan importante.

El verdadero desafío de las redes inalámbricas Wi Fi consiste en proveer a cada usuario el ancho de banda suficiente para llevar a cabo, de manera eficiente, sus labores.

Tomando en cuenta lo anterior, al realizar un diseño de red personal para el acceso a Internet, habrá que tomar en cuenta el alcance de la red, el cual dependerá de:

- La potencia del Punto de Acceso.
- La potencia del accesorio o dispositivo Wi-Fi por el que nos conectamos.
- Los obstáculos que la señal tenga que atravesar (muros o metal).

Cuanto más lejos (linealmente) quieras llegar, más alto deberás colocar el Punto de Acceso. Muchos de los actuales Puntos de acceso vienen preparados para poderlos colgar en la pared.

También hay que observar las siguientes consideraciones:

- Si quieres llegar lejos, evita también interferencias como microondas o teléfonos inalámbricos.
- Si la señal te llega debilitada, utiliza un amplificador de señal o si es posible, montar una nueva antena de más potencia al Punto de acceso (los Puntos de Acceso de gama baja NO lo permiten) o una antena exterior al accesorio (normalmente sólo para formatos PCMCIA o PCI).

CONCLUSIONES

CONCLUSIONES

La funcionalidad y eficiencia de cualquier tipo de red depende de las necesidades muy particulares de los usuarios y del uso que éstos le den.

Si bien las redes cableadas son muy eficientes, las redes Wireless (inalámbricas), con todas sus características, son una realidad que no podemos pasar por alto.

Sabemos que, al comparar un tipo de red con el otro, encontraremos infinidad de diferencias; lo que las hace compatibles es su objetivo: Hacer más eficiente la transferencia de información y la comunicación entre los usuarios.

Las redes inalámbricas, a pesar de ser más lentas que las redes cableadas, han abarcado gran parte del mercado de las comunicaciones; una de las razones de este suceso es la portabilidad que ofrecen, al poder ubicarlas en cualquier lugar; asimismo, la facilidad en su configuración.

En un futuro, se espera que ambas tecnologías (la cableada y la inalámbrica) puedan fusionarse en sistemas híbridos que ofrezcan las ventajas de cada tecnología; incrementando así la eficiencia y comodidad.

APÉNDICE:

ESTÁNDARES PARA REDES INALÁMBRICAS

ESTÁNDARES IEEE
PARA REDES INALÁMBRICAS

Estándar 802.11

Fue el primero de los estándares desarrollados por la IEEE para tecnologías de redes inalámbricas (wireless). Permite la conexión de dispositivos móviles (como lap tops, Palm, teléfonos celulares conectados a una red cableada por medio de un punto de acceso). La conexión se realiza a través de ondas de radio-frecuencia. Originalmente, ofrecía una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de 2.4 GHz. Se le conoce popularmente como Wi Fi. Tiene un área de cobertura de cien metros aproximadamente. Ofrecían velocidades muy pequeñas y no permitían implementar aplicaciones empresariales muy robustas; por lo tanto, se crearon nuevos grupos de trabajo para crear otros estándares.

Estándar 802.11a

Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz; por lo tanto, no es compatible con los estándares 802.11b y 802.11g. Utiliza la tecnología OFDM (Orthogonal Frecuency Division Multiplexing). Esta banda de 5 GHz no se pudo utilizar, al comienzo, en muchos países, puesto que estaba asignada a las tareas de las fuerzas y organismos de seguridad; sin embargo, últimamente está siendo liberada.

Estándar 802.11b

Estándar de conexión wireless, que suministra una velocidad de transmisión máxima de 11 Mbps y opera en una banda de 2.4 GHz. Es el más popular puesto que fue el primero en imponerse y existe un inventario muy grande de equipos y dispositivos que manejan esta tecnología (Tecnología DSS, Direct Sequencing Spread). Es compatible con el estándar 802.11g, lo que permitió la incorporación de éste último a las redes inalámbricas ya existentes. No es compatible con el estándar 802.11a, pues funciona en otra banda de frecuencia.

Estándar 802.11e

Este estándar se encuentra en elaboración desde junio de 2003, está destinado a mejorar la calidad de servicio en Wi Fi (QoS, Quality of Service). Es de suma importancia para la transmisión de voz y vídeo. Sin embargo, aún se encuentra solamente en borrador.

Estándar 802.11g

Estándar de conexión wireless que suministra una velocidad de transmisión máxima de 54 Mbps y opera en una banda de frecuencia de 2.4 GHz.. Se basa en la tecnología OFDM, al igual que el estándar 802.11a. Es compatible con el estándar 802.11b; sin embargo, al mezclar equipos del estándar 802.11b con equipos del estándar 802.11g, la velocidad de transmisión la fija el equipo más lento.

Estándar 802.11i

Estándar de seguridad para redes Wi FI, aprobado a mediados de 2004. Se desarrolló en dos fases: el protocolo WPA y el protocolo WPA2. Funciona con los puntos de acceso y dispositivos Wi Fi existentes.

Estándar 802.11n

Es un estándar nuevo que aún se encuentra en elaboración, desde enero de 2004. Su objetivo es elaborar un estándar con velocidades de transmisión superiores a 100 Mbps.

Estándar 802.16

Estándar de transmisión wireless conocido como WIMAX (Worldwide Interoperability for Microwave Access). Es compatible con WIFI. Se originó en Abril de 2002 con la finalidad de cubrir inalámbricamente distancias de hasta 50 Km. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz.. La interoperatividad es certificada por el WIMAX FORUM

Estándar 802.16d

Estándar de transmisión wireless (WIMAX) que suministra una velocidad de entre 300 K y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Ratificado a finales de 2004. Se utiliza para el cubrimiento de la "primer milla". WIMAX: Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal

Estándar 802.1x

Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.
El estándar 802.1x constituye la columna vertebral de la seguridad Wi Fi y es imprescindible y muy recomendable su utilización en toda red empresarial que pretenda lograr una seguridad robusta. Este estándar introduce importantes cambios en el esquema de seguridad Wi Fi. En el esquema 802.1x se autentica al usuario y no al dispositivo.

ORGANIZACIONES

WIMAX

WIMAX (estándar IEEE 802.16 y sus variantes) es una tecnología inalámbrica (Wireless), complementaria de Wi Fi y que ha sido concebida y desarrollada para suministrar servicios de banda ancha a campus universitarios, urbanizaciones, etcétera, en tramos de pocos kilómetros (3 a 10 kilómetros, aunque pueden alcanzar más de 40 kilómetros).

Los estándares Wi Max aprobados y que se están comenzando a utilizar son:

ESTÁNDAR WI MAX	FECHA DE APROBACIÓN	FRECUENCIA	FINALIDAD
IEEE 802.16	Diciembre, 2001	10 – 66 GHz	
IEEE 802.16a	Enero, 2003	2 – 11 GHz	Banda ancha fija
IEEE 802.16-2004	Junio, 2004	2 – 11 GHz	Soporte para usuarios
IEEE 802.16-2005	Diciembre, 2005	2 – 11 GHz (<6 GHz)	Añadir movilidad

La organización que regula, homologa y certifica los productos Wi Max se llama WIMAX Forum y tiene características similares a la Wi Fi Alliance. Sólo los equipos y dispositivos que sean “WIMAX Forum Certified” aseguran una compatibilidad probada con equipos y dispositivos de otras marcas.

Bluetooth

Bluetooth (Estándar IEEE 802.15) es una tecnología inalámbrica de corto alcance orientada a la transmisión de voz y datos. Funciona en la banda de frecuencia de 2.4 GHz que no requiere licencia y tiene un alcance de 10/100 metros dependiendo de los dispositivos.

La organización que regula y promueve la tecnología Bluetooth es el SIG (Special Interest Group). Su función es la de desarrollar la tecnología y coordinar a los miles de fabricantes que la incluyen en sus productos.

WI FI

Wi Fi es el nombre comercial del estándar IEEE 802.11; es una tecnología novedosa y práctica que se está difundiendo muy rápido en todo el planeta. Es una tecnología inmadura que va requiriendo nuevos estándares o modificaciones en los estándares existentes, a medida que van apareciendo inconvenientes.

A partir del estándar IEEE 802.11/Wi Fi, se fueron desarrollando otros estándares relacionados con Wi Fi, los cuales han ido introduciendo mejoras y solucionando inconvenientes.

GLOSARIO

802.11	Conjunto de estándares de red de área local inalámbrica definidos por el IEEE.
ACCESS POINT	Punto de acceso. Dispositivo que normalmente se conecta a los dispositivos de cliente. Tiene un punto Ethernet y otro de energía; e incluye uno o dos antenas que transmiten y reciben señales RU.
ACCESO REMOTO	Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.
ACCESORIO WI FI	Es el accesorio adicional que usaremos para incoporar el estándar 802.11 a nuestro equipo (PDA, ordenador portátil o de sobremesa), en caso de no tener Wi-Fi integrado. Estos accesorios pueden encontrarse en formato de tarjetas PCMCIA (para portátil), PCI y USB (para ordenador de sobremesa) y esperamos que muy pronto en formato SD (Secure Digital) para nuestros PDAs Palm OS.
AD-HOC	(Punto a Punto) Modo de conexión en una red wireless que define que nuestro equipo (PDA, ordenador portátil o de sobremesa) se conectará directamente a otro equipo, en vez de hacerlo a un Punto de Acceso. Ad-Hoc es una forma barata de tener conexión a Internet en un segundo equipo (por ejemplo un PDA) sin necesidad de comprar un Punto de Acceso. Para este uso la configuración se dificulta ya que tenemos que configurar en el ordenador que tiene la conexión a Internet un programa *enrutador* o una conexión compartida.
ADMINISTRADOR	Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local o de un servidor de red.
ADMINISTRACIÓN DE RED	Término que se usa para describir sistemas o acciones que ayudan a mantener Y caracterizar una red; o resolver problemas de la red.
AMPLIFICADOR	Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido pre-amplificado y un amplificador lineal de salida de radio frecuencia (RF).

ANCHO DE BANDA	Rango de frecuencia necesaria para transportar una señal, medido en unidades de Hertz (HZ). Depende del esquema de modulación, velocidad de datos y cantidad de canales del espectro de radio.
ANSI	Acrónimo del Instituto Nacional de estándares de Estados Unidos. Una organización voluntaria compuesta de miembros corporativos, gubernamentales y de otros tipos, que coordina las actividades relacionadas con los estándares internacionales y de la Unión Americada relacionados, entre otras cosas, con las comunicaciones y las redes.
ANTENA	Dispositivo para transmitir o recibir una frecuencia de radio (RU); están diseñadas para frecuencia específicas y de manera relativamente estricta.
ARPANET	Red pionera de gran alcance fundada por ARPA (Advanced Research Projects Agency) después DARPA. Sirvió de 1969 a 1990 como base para las primeras investigaciones de red durante el desarrollo de Internet. ARPANET consiste en nodos individuales conmutadores de paquetes interconectados por líneas arrendadas.
ASCII	Código estándar de Estados Unidos para el intercambio de información. Especifica un código de ocho bits para la representación de caracteres.
ATENUACIÓN	Pérdida de energía en la señal de comunicación; sea por el diseño del equipo, manipulación del operador o transmisión a través de un medio.
AUTENTICACIÓN	Verificación de la identidad de una persona o proceso. Es abierta si se verifica a una persona; es de estación si lo que se verifica es un dispositivo.
BANDA BASE	Banda angosta, característica de una tecnología de red donde solamente se usa un portador de frecuencia.
BANDA DE PASO	Se le denomina a las frecuencias que un radio permite que pasen desde su entrada hasta su salida.
BIT	Es la unidad más pequeña de información que puede controlar una computadora. Es un dígito binario; es decir, un cero o un uno.

BLUETOOTH	Tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de diez). No está pensada para soportar redes de ordenadores, sino para comunicar un ordenador o un dispositivo con sus periféricos.
BPSK	Acrónimo de la modulación de fase por desplazamiento binario. Se trata de una técnica de modulación de frecuencia digital que se usa para transmitir información.
BRIDGE	Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar
BSS	Basic Service Set. Conjunto de servicios básicos. Es una modalidad de comunicación en las que se puede configurar las terminales de una red Wi Fi. También es conocido como modo infraestructura.
BYTE	Conjunto de ocho bits. Representa un carácter alfabético o numérico.
CCK	Complementary Code K-ying Salto de código complementario. Es una técnica de modulación utilizada en Wi Fi junto con las técnicas de espectro distribuido.
CERTIFICADO	Una declaración firmada en forma digital de una entidad que establece que una clave pública en alguna entidad tiene algún valor en particular.
CLAVE	Se usa para abrir un texto cifrado. La clave se puede considerar en los mismos términos relativos que un cerrojo o una llave. Una sola clave puede generar una gran cantidad de versiones diferentes de texto cifrado desde el texto sencillo.
CLAVE DE ENCRIPTACIÓN	Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

CLAVE DE REGISTRO	El registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiarán de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.
CONMUTACIÓN DE PAQUETES	Método que consiste en dividir toda la información que sale de un ordenador para ser trasmitida por la red en bloque de determinada longitud (Paquetes) que contienen la información relacionada con el origen y destino del paquete así como el orden que ocupa dentro de la división realizada. Esto permite que cada paquete se mueva de forma independiente en la red y al llegar a su destino puedan ser reensamblados para construir nuevamente la información enviada.
CORTAFUEGOS	Firewall. Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc...
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance. Acceso múltiple por detección de portadora con evitación de colisión. Es el sistema que emplea Wi Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión)
DESENCRIPTAR	Proceso de transformación de ciphertext - texto encriptado o cifrado - a plaintext. Es la acción inversa a encriptar.
DHCP:	Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente. Por defecto la mayoría de los routers ADSL y los Puntos de Acceso tienen DHCP activado.

DISPOSITIVO MÓVIL	Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras,...).
DIRECCIÓN MAC:	(MAC address - Media Access Control address) Es el código único de identificación que tienen todas las tarjetas de red. Nuestro accesorio Wi-Fi o nuestro PDA con Wi-Fi integrado, al ser un dispositivo de red, también tendrá una dirección MAC única. Las direcciones MAC son únicas (ningún dispositivo de red tiene dos direcciones MAC iguales) y permanentes (ya que vienen preestablecidas de fábrica y no pueden modificarse).
DSSS	Espectro Amplio mediante Secuencia Directa. A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos .Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.
ESTÁNDAR	Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etcétera.
ETHERNET	Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

FHSS	Espectro Amplio mediante Saltos de Frecuencia. Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar acabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este "Hopping Pattern". El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.
FIRMA ELECTRÓNICA	El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.
FIRMWARE	Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es un combinación de software y hardware. ROMs, PROMs e EPROMs que tienen datos o programas grabados dentro son firmware.
FTP	Protocolo de transferencia de archivos que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.
GATEWAY	Puerta de enlace Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas
HARDWARE (MAQUINARIA)	Componentes físicos de una computadora o de una red, a diferencia de los programas o elementos lógicos que los hacen funcionar.
HOTSPOT	Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc...) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

HUB	(concentrador) Dispositivo electrónico al que se conectan varios ordenadores, por lo general mediante un cable de par trenzado. Un concentrador simula en la red que interconecta a los ordenadores conectados.
IEEE	Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Es la sociedad que se encarga de los estándares de redes a nivel internacional.
INFRAESTRUCTURA	Modo de conexión en una red wireless que define que nuestro equipo (PDA, portátil u ordenador de sobremesa) se conectará a un Punto de Acceso. El modo de conexión deberá de especificarse en la configuración de nuestro equipo o del accesorio Wi-Fi. Por defecto viene activado este modo.
INTEGRIDAD DE ARCHIVOS	Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).
INTERNET	Conjunto de redes y ruteadores que utiliza los protocolos TCP/IP para formar una sola red virtual cooperativa.
IP ADDRESS	Dirección IP. Una dirección IP es una serie de números que identifica a nuestro equipo dentro de una red. Distinguimos entre IP pública (ej. 80.20.140.56), cuando es la dirección que nos identifica en Internet (por ejemplo la IP de tu router ADSL en Internet) e IP privada (ej. 192.168.0.2), que es la dirección que identifica a un equipo dentro de una red local (LAN). Si, por ejemplo, pensamos en una red local con un router ADSL, los PCs o equipos conectados a la red tendrán sólo IP privada, mientras que el router tendrá una IP pública (su identificación en Internet) y una IP privada (su identificación en la red local).

LAN	Red de área local. Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topologia en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.
MAC	Dirección de Control de Acceso a Medios. Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexademinal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.
MBPS	Megabits por segundo. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.
MHz	Mega hertz. Unidad empleada para medir la "velocidad bruta" de los microprocesadores equivalente a un millón de hertzios.
MODEM	Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).
PROTOCOLO	Descripción formal de formatos de mensajes y reglas que dos o más ordenadores deben seguir para intercambiar mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de ordenador a ordenador o el intercambio entre programas de aplicación.
PUNTO DE ACCESO	Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

ROUTER	Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.
ROAMING	En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad
SERVIDORES DNS	DNS server Las páginas web también tienen su dirección IP pública y es a través de ésta dirección como en realidad nos conectamos a ellas. Pero claro, es más sencillo memorizar o escribir el nombre del dominio que su dirección IP. Para no memorizar la retahíla de números tenemos los servidores DNS. Un servidor DNS es un servidor en donde están almacenadas las correlaciones entre nombres de dominio y direcciones IP. Cada vez que cargamos una página web, nuestro equipo (PDA, portátil u ordenador de sobremesa) envía una petición al servidor DNS para saber la dirección IP de la página que queremos cargar, y es entonces cuando hace la conexión. Probablemente se esta familiarizado con eso de "servidor DNS primario" y "servidor DNS secundario". El primario es el "principal" y el secundario es el de emergencia que usará nuestro ordenador en caso de que el primario no funcione.
SISTEMA OPERATIVO	Conjunto de programas o software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera eficiente.
SOFTWARE	Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica de una computadora.
SSID	Service Set Identification Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso.

SUBNET ADDRESS	Máscara de subred: () Cifra de 32 bits que especifica los bits de una dirección IP que corresponde a una red y a una subred. Normalmente será del tipo 255.255.255.0
SWITCH	(interruptor o conmutador). Dispositivo de interconexión de redes de ordenadores. Un switch interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo con la dirección de destino de los datagramas en la red. Los switches se utilizan cuando se desea conectar múltiples redes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las mismas.
TARJETA DE RED INALÁMBRICA	Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB
TEXTO CODIFICADO	Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo.
TCP/IP	Protocolo que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes.
VPN	Red Privada Virtual. Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (*LAN*).
WAN	Red de cobertura amplia. Tipo de red compuesta por dos o más redes de área local (LANs) conectas entre si vía teléfono (generalmente digital).
WI FI ALLIANCE	Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado .

WPA	WPA - Protocolo de Seguridad en redes Inalámbricas. Protocolo de Seguridad para redes inalámbricas. Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i
WPA2	Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.
WEP	(Wired Equivalent Privacy) Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.
WI FI	WiFi es el nombre comercial del estándar IEEE 802.11. Es una tecnología novedosa y práctica que se está difundiendo rápidamente por todo el planeta. No obstante, es una tecnología inmadura, que requiere de nuevos estándares, cada vez, o modificaciones de los ya existentes, en la medida en que van apareciendo inconvenientes.
WIMAX	Worldwide Interoperability for Microwave Access. Grupo no lucrativo formado en abril de 2003 iniciativa de Intel/Nokia/Fujitsu/entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica
WLAN	También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA	Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

- Black, Wyless. Redes de computadores, protocolos, normas e intérpretes. Ed. Alfaomega

- Carballar, José A. Wi Fi. Como construir una red inalámbrica. Ed. Alfaomega.

- Comer, Douglas. Redes globales de información con Internet y TCP/IP. Principios básicos, protocolos y arquitectura. Tomos I y II. Editorial Pueblo y Educación. La Habana, 2005

- Engst, Adam – Fleishman, Glenn. Ed. Anaya Multimedia.

- Reid, Neild – Seide, Ron. 802.11 Wi Fi. Manual de redes inalámbricas. Ed. Mc Graw Hill

- Singhal, Hura. Data Computer Comunications. Ed. CCr, Press

- Tanenbaum, Andrew. Redes de computadoras. Ed. Pearson.

- Yañez, José. Redes, comunicación y el laboratorio de informática. Editorial Pueblo y Educación. La Habana, 2002.

FUENTES

http://www.monografias.com

http://www.geocities.com/Eureka/Plaza/2131/primeras.html

http://www.geocities.com/nicaraocalli/

OBJETIVOS

- Mostrar las formas más comunes en la transmisión de información utilizando redes informáticas
- Determinar las características de las redes inalámbricas, así como las recomendaciones en su uso y diseño.
- Marcar las bases de diseño de redes inalámbricas para uso personal.
- Especificar los errores comunes en el diseño de redes inalámbricas, como advertencia de lo que debe evitarse.

JUSTIFICACIÓN

Teniendo en cuenta la importancia y la evolución en las comunicaciones y la transmisión de información, es importante hacer notar que una opción muy aceptable es el uso y manejo de las redes inalámbricas.