CAPÍTULO I
ANTECEDENTES

1.1 Conceptos de una red de datos.

1.1.1 Red de computadoras.

Una red de computadoras (también llamada red de datos) es un conjunto de computadoras y/o dispositivos conectados por enlaces, a través de medios físicos (medios guiados) o inalámbricos (medios no guiados) y que comparten información (archivos), recursos (CD-ROM, impresoras, etcétera.) y servicios (e-mail, chat, juegos), etcétera.

1.1.2 Medios de Transmisión.

Normalmente son utilizados tres tipos de cables en las redes locales:

1.1.2.1 Coaxial.

Tiene un gran ancho de banda. Tiene una baja sensibilidad a EMI (Electromagnetic Interference). Se pueden alcanzar longitudes moderadas (200 a 300 mts) y es de costo mediano.

Usa un conector tipo T para conectar los dispositivos al medio. También puede usar un transceiver para tener una entrada tipo AUI (Attachment Unit Interface). El transceiver tiene que ser compatible respecto a la frecuencia a la que trabaja la red.

Hay dos tipos de cable coaxial:

- Cable fino (Thinnet).
- Cable grueso (Thicknet).

El tipo de cable coaxial más apropiado depende de las necesidades de la red en particular.

El cable Thinnet es un cable coaxial flexible de unos 0,64 centímetros de grueso (0,25 pulgadas). Este tipo de cable se puede

utilizar para la mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.

El cable coaxial Thinnet puede transportar una señal hasta una distancia aproximada de 185 metros (unos 607 pies) antes de que la señal comience a sufrir atenuación.

1.1.2.2 Fibra óptica.

En un cable de fibra óptica, la fibra óptica lleva las señales digitales (datos) en la forma de pulsos modulados de luz. Ésta es una forma relativamente segura de enviar datos ya que no hay impulsos eléctricos dentro del cable de fibra óptica. Esto significa que la fibra óptica no puede ser "espiada" y los datos robados, que sí se puede hacer con los cables de cobre que llevan los datos como señales electrónicas.

El cable de fibra óptica es bueno para transmisiones muy rápidas y de alta capacidad debido a su carencia de atenuación y a la fidelidad de la señal. La fibra óptica consiste en un cilindro de vidrio extremadamente delgado, llamado el núcleo, rodeado por una cubierta concéntrica de vidrio, conocida como cladding. A veces la fibra está hecha de plástico. El plástico es más fácil de instalar, pero no puede llevar los pulsos de luz tan lejos como el vidrio.

Cada fibra pasa las señales en sólo una dirección, así que el cable consiste de dos o más fibras en cubiertas separadas. Uno para recibir y otro para enviar. Una capa de plástico de refuerzo rodea cada fibra y le da flexibilidad. Por último una capa de kevlar le provee de fuerza.

Tipos de fibra óptica.

Básicamente, existen dos tipos de fibra óptica: multimodo y monomodo.

Fibra óptica multimodo.

Este tipo de fibra fue el primero en fabricarse y comercializarse. Su nombre proviene del hecho de que transporta múltiples modos de forma simultánea, ya que este tipo de fibra se caracteriza por tener un diámetro del núcleo mucho mayor que las fibras monomodo.

El mayor diámetro del núcleo facilita el acoplamiento de la fibra, pero su principal inconveniente es que tiene un ancho de banda reducido como consecuencia de la dispersión modal. Los diámetros de núcleo y cubierta típicos de estas fibras son 50/125 y 62,5/125 mm.

La fibra óptica multimodo es adecuada para distancias cortas, como por ejemplo redes LAN o sistemas de video vigilancia.

Fibra óptica multimodo índice escalonado.

En este tipo de fibra óptica viajan varios rayos ópticos simultáneamente. Éstos se reflejan con diferentes ángulos sobre las paredes del núcleo, por lo que recorren diferentes distancias, y se desfasan en su viaje dentro de la fibra, razón por la cual la distancia de transmisión es corta.

Hay que destacar que hay un límite al ángulo de inserción del rayo luminoso dentro de la fibra óptica, si este límite se pasa el rayo de luz ya no se reflejará, sino que se refractará y no continuará el curso deseado (Figura 1.1).

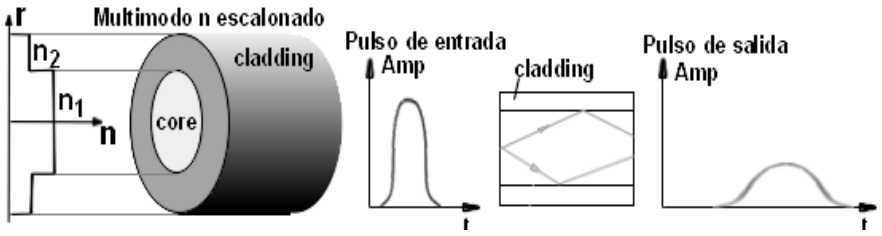


Figura 1.1 Fibra óptica multimodo índice escalonado.

Fibra óptica multimodo índice gradual.

En este tipo de fibra óptica, el núcleo está constituido de varias capas concéntricas de material óptico con diferentes índices de refracción, causando que el rayo de luz de refracte poco a poco mientras viaja por el núcleo.

En estas fibras el número de rayos ópticos diferentes que viajan es menor que en el caso de la fibra multimodo índice escalonado y por lo tanto, su distancia de propagación es mayor (Figura 1.2).

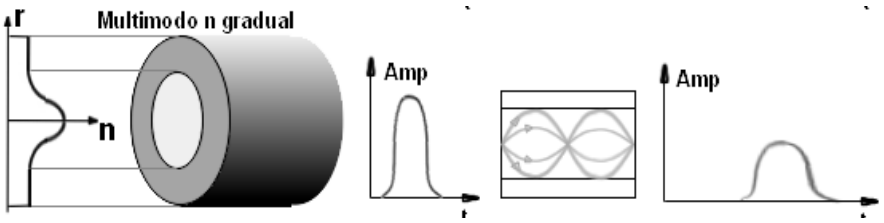


Figura 1.2 Fibra óptica multimodo índice gradual.

Fibra óptica monomodo.

Las fibras ópticas monomodo tienen un diámetro del núcleo mucho menor, lo que permite que se transmita un único modo y se evite la dispersión multimodal. Los diámetros de núcleo y cubierta típicos para estas fibras son de 9/125 mm.

Las fibras monomodo también se caracterizan por una menor atenuación que las fibras multimodo, aunque como desventaja resulta más complicado el acoplamiento de la luz y las tolerancias de los conectores y empalmes son más estrictas. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit, las cuales vienen limitadas principalmente por la dispersión cromática y los efectos no lineales.

Los diámetros de núcleo y cubierta típicos para estas fibras son de 9/125 mm.

La fibra óptica monomodo está diseñada para sistemas de comunicaciones ópticas de larga distancia (Figura 1.3).

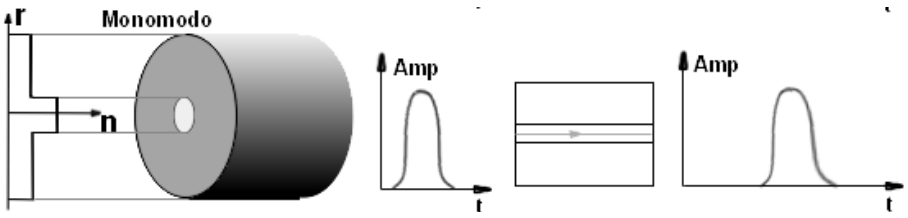


Figura 1.3 Fibra óptica monomodo.

Tipos de conectores para fibra óptica.

Éstos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor. Los tipos de conectores disponibles son muy variados, entre los que se pueden encontrar están los siguientes (Figura 1.4):

- FC, que se usa en la transmisión de datos y en las telecomunicaciones.
- FDDI, se usa para redes de fibra óptica.
- LC y MT-Array que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC se usa en redes de edificios y en sistemas de seguridad.

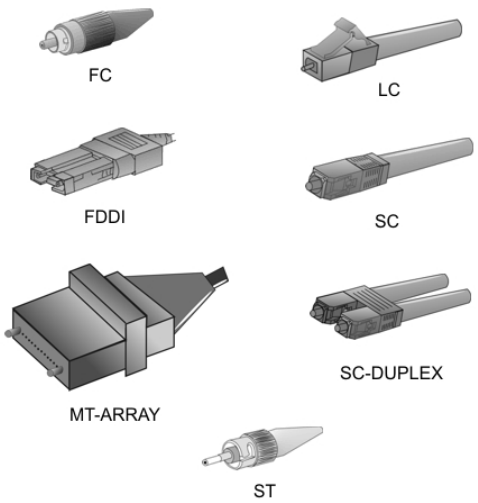


Figura 1.4 Tipos de conectores para fibra óptica.

1.1.2.3 Par trenzado.

Un cable de par trenzado es uno de los tipos de cables de pares compuesto por hilos, normalmente de cobre, trenzados entre sí. Hay cables de 2, 4, 25 o 100 pares de hilos e incluso de más. El trenzado mantiene estable las propiedades eléctricas a lo largo de toda la longitud del cable y reduce las interferencias creadas por los hilos adyacentes en los cables compuestos por varios pares.

Aún teniendo trenzado a veces es necesario apantallar estos cables con un recubrimiento metálico o incluso apantallar cada par trenzado dentro del cable completo para evitar interferencias entre éstos. Definimos 3 tipos básicos de pares trenzados según su recubrimiento:

- UTP: (Unshielded Twisted Pair) Sin ningún tipo de recubrimiento metálico.
- STP: (Shielded Twisted Pair) Recubrimiento metálico alrededor del cable completo.
- S/STP: (Screened STP) Recubrimiento metálico alrededor de cada par trenzado y del cable completo.

Categorías de UTP.

Las Categorías de UTP se muestran en la Tabla 1.1.

Tabla 1.1 Categorías de UTP.

Categoría	Características
1	Se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos, trabaja en una frecuencia de 4 MHz.
2	Puede transmitir datos a velocidades de hasta 4 Mbps, trabaja en una frecuencia de 5 MHz.
3	Se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps, trabaja en una frecuencia de 16 MHz.

4	Se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps, trabaja en una frecuencia de 20 MHz.
5	El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps, trabaja en una frecuencia de 100 MHz.
5e	Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque sí está diferenciada por los diferentes organismos.
6	Puede transmitir velocidades de hasta 1000 Mbps, trabaja en una frecuencia de 250 MHz.
7	Esta categoría no está estandarizada, se espera que cumpla los requisitos exigidos para el nuevo estándar 10GBaseT. Se supone que no utilizará el viejo conector RJ45, ya que la propuesta es utilizar un conector Nexans GG45 que es compatible con los RJ45. La novedad es que el nuevo conector tiene la apariencia de un RJ45 de 8 conectores al que se le han añadido 4 en la parte inferior.

1.1.3 Cableado estructurado.

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. Las características e instalación de estos elementos se debe hacer en cumplimiento de estándares para que califiquen como cableado estructurado.

El propósito del cableado estructurado, es el de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

1.1.3.1 Subsistema de cableado estructurado.

Una solución de cableado estructurado se divide en una serie de subsistemas. Cada subsistema tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada para cada caso (Figura 1.5).

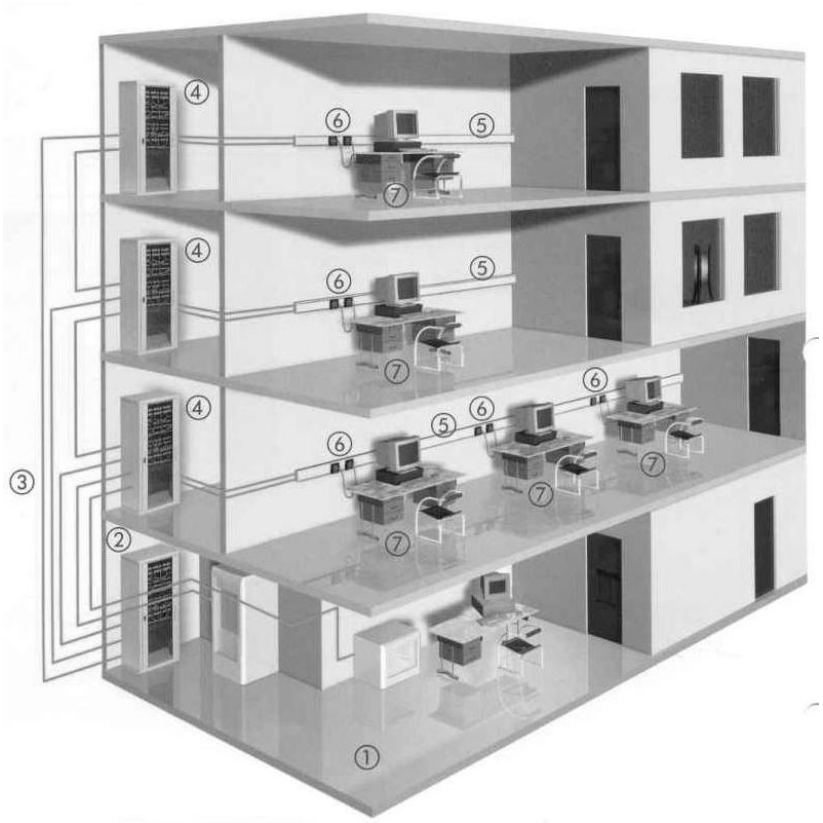


Figura 1.5 Subsistema de cableado estructurado.

1. Subsistema de administración.
2. Rack Principal.
3. Cableando horizontal.
4. Rack de planta.
5. Cableando vertical.
6. Tomas de usuario.
7. Área de trabajo.

1. Subsistema de administración.

En este subsistema se incluyen todos los componentes que se colocan dentro del cuarto de administración del piso y que permiten la conexión y administración de las distintas plantas que conforman el edificio o campus. Aquí encontramos los

bloques de conexión de diferentes tipos de cables y conectores por ejemplo, paneles de conexión tipo RJ45, las cajas terminales de acometida de fibra óptica con conectores adecuados, los armarios o rack's que sirven para la fijación de equipo de comunicación como podrían ser switch, hub, organizadores, patch panel, etcétera.

2. Rack principal.

En este rack o bastidor se aloja el equipo electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante. Se encuentran los dispositivos y equipos que alimentaran al edificio o campus, en este está instalada la acometida principal, que da acceso a internet.

3. Cableado horizontal.

Este subsistema comprende el conjunto de medios de transmisión (cables, fibras, coaxiales, etcétera.) que unen el rack de planta con el conector o conectores del área de trabajo, este cableado generalmente no debe ser mayor de 100 metros. Ésta es una de las partes más importantes a la hora del diseño debido a la distribución de los puntos de conexión o tomas de usuario.

En este subsistema se estudian y definen las rutas más adecuadas para distribuir la totalidad del cableado a lo largo de un piso. Estas rutas deben ajustarse a las distancias definidas por las normas. Igualmente se determina el tipo de elemento a utilizar para transportar el cable, de manera segura y confiable, con la capacidad suficiente y con el espacio requerido para crecimientos futuros. Entre los diferentes tipos de medios de transporte tenemos las bandejas de aluminio o de lámina, tuberías metálicas, ductos metálicos o en mampostería, canaletas perimetrales o por cielo raso, escalerillas, etcétera. En la instalación de estos

elementos, se deben cumplir diferentes aspectos de las normas respectivas, especialmente en lo relacionado con la capacidad de los mismos, materiales, curvaturas máximas, cantidad de cajas de paso, etcétera.

4. Rack de planta.

Este rack de planta ayuda a interconectar el rack principal con cada piso y de esta forma poder tener comunicación en cada piso del edificio o campus.

5. Cableando vertical.

Este subsistema está encargado de interconectar todos los subsistemas de cada piso a lo largo del edificio. Esta interconexión consiste en conectar los armarios de cada piso, con cables definidos para la aplicación diseñada.

Este subsistema puede estar compuesto por diferentes tipos de cables de acuerdo con el número de salidas de información que se tengan en cada piso. Generalmente se conectan siguiendo una topología en estrella estando el centro de la estrella en el cuarto principal de administración del sistema. En resumen, a través de estos cables (UTP, fibra o multipar) se llevan las señales de las aplicaciones definidas para el sistema (voz, datos, seguridad, video, etcétera.) desde el cuarto principal hasta dejarlas disponibles en cada piso.

Aquí se encuentra también todo lo relacionado con los ductos o espacios físicos con que la edificación cuenta para realizar esta distribución. Se tiene ductos o perforaciones en las placas, escalerillas metálicas, tuberías, etcétera.

6. **Tomas de usuario.**

En cada planta se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada piso.

7. **Áreas de trabajo.**

El subsistema de área de trabajo, son las conexiones que se tienen dentro de la red desde la roseta hacia cualquier equipo ya sea una computadora, una cámara de seguridad, una impresora, una alarma, etcétera.

1.1.4 Topologías.

La topología de red es la disposición física en la que se conecta una red de computadoras.

1.1.4.1 Tipos de topologías.

Las principales topologías son:

- **Red en Bus.**

En una topología de bus (Figura.1.6), cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma.

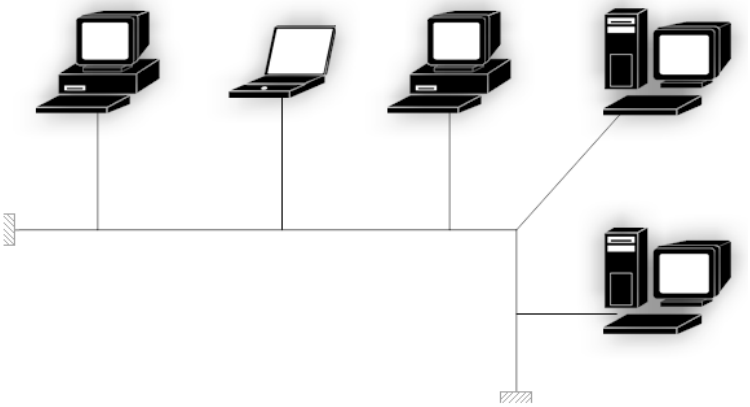


Figura 1.6 Topología de red bus.

- **Red en anillo.**

Una topología de anillo (Figura.1.7), consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o token.

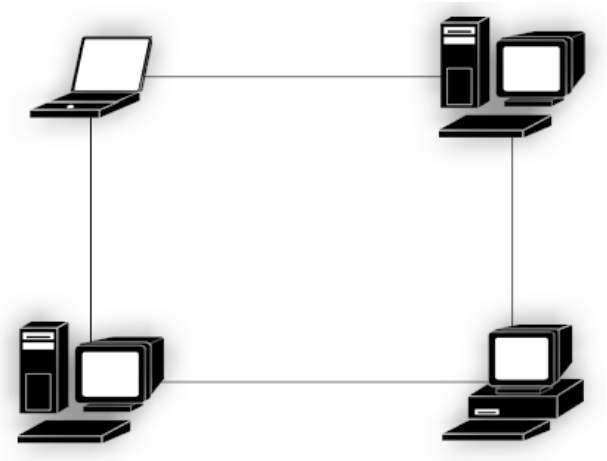


Figura 1.7 Topología de red anillo.

- **Red en estrella.**

Uno de los tipos más antiguos de topologías de redes es la estrella (Figura.1.8), la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos.

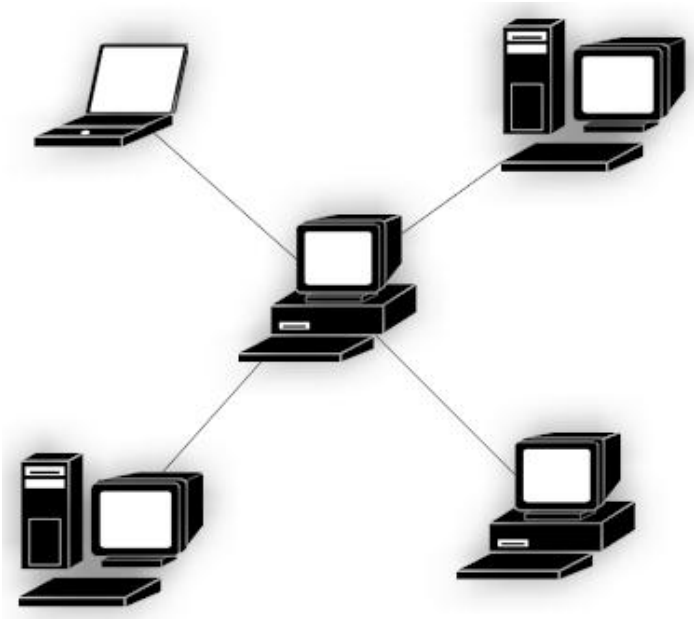


Figura 1.8 Topología de red estrella.

1.1.5 Servidores.

En una red de datos, un servidor es un equipo que pone ciertos recursos a disposición de otras computadoras (los clientes). Estos recursos pueden ser datos, aplicaciones, impresoras, etcétera.

Un servidor no es necesariamente una máquina de última generación grande y monstruosa, no es necesariamente un supercomputadora; un

servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente.

1.1.5.1 Tipos de servidores.

Entre los servidores más conocidos se encuentran:

- **NAT.**

El NAT (Network Address Translation, en español Traducción de la dirección de red) es una aplicación no técnica y sencilla que determinado dispositivo o aplicación software es capaz de cambiar la dirección IP de origen o destino por otra dirección definida previamente. Se puede utilizar para dar salida a redes públicas a computadoras que se encuentran con direccionamiento privado o para proteger máquinas públicas.

- **Bridge.**

Un dispositivo que conecta dos o más redes físicas y sirve para transmitir paquetes entre ellas. Puede utilizarse también para filtrar los paquetes que entran o salen, selectivamente.

- **Proxy.**

La palabra proxy se usa en muchas situaciones en donde tiene sentido un *intermediario*.

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

El servidor proxy de web (comúnmente conocido solamente como "proxy"). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etcétera.

- **DHCP.**

El DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Provee los parámetros de configuración a las computadoras conectadas a la red informática con el protocolo TCP/IP (Máscara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- ✓ *Asignación manual o estática*: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

- ✓ *Asignación automática*: Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

- ✓ *Asignación dinámica*: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

- **Servidor Web.**

Un servidor web es un programa que implementa el *protocolo HTTP* (*hypertext transfer protocol*). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

Un servidor web se encarga de mantenerse a la espera de *peticiones HTTP* llevada a cabo por un *cliente HTTP* que solemos conocer como *navegador*. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita.

- **Servidor de base de datos.**

Un servidor de base de datos es un equipo de cómputo que cuenta con una aplicación que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

- **Servidor Radius.**

Un servidor RADIUS centraliza una base de datos de usuarios y passwords y espera que equipos como access servers le pregunten si cierto usuario con cierto password tiene acceso. El servidor RADIUS recibe no solo usuario y password sino una multitud de atributos, como el puerto del access server a donde el usuario se está conectando, y debe responder si se le permite al usuario conectarse, junto con una serie de atributos que pueden ir desde la dirección IP a asignarle al usuario, protocolos a utilizar o reglas de filtrado de paquetes.

1.1.6 Modelo OSI.

1.1.6.1 Historia.

Al principio, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de trabajar en red, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban este tipo de tecnología de trabajo en red. Las tecnologías de trabajo en red que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de trabajo

en red como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

1.1.6.2 Modelo de referencia OSI.

Siguiendo el esquema de este modelo se crearon numerosos protocolos, por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo, sigue siendo muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones (sin importar su poca correspondencia con la realidad).

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

- **Capa Física (Capa 1).**

  La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (por ejemplo tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etcétera.) y la forma en la que se transmite la información (codificación de señal, niveles de

tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etcétera).

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es unidireccional o bidireccional (símplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etcétera.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

- **Capa de enlace de datos (Capa 2).**

  Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

  La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

  Se hace un direccionamiento de los datos en la red ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores, de la topología de la red.

- **Capa de red (Capa 3).**

  El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan en español encaminadores, aunque es más

frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande).

El switch también puede trabajar en esta capa dependiendo de la función que se le asigne.

- **Capa de transporte (Capa 4).**

  Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a

3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Se puede definir a la capa de transporte como:

Capa encargada de efectuar el transporte de los datos de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.

- **Capa de sesión (Capa 5).**

  Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

  - Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
  - Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
  - Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.
  - Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

    En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén trasmitiendo archivos.

- **Capa de presentación (Capa 6).**

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

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

  Por lo tanto, se define a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

  Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

- **Capa de aplicación (Capa 7).**

  Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

  Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con

programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol).
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros.
- SMTP (Simple Mail Transfer Protocol), envío y distribución de correo electrónico.
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final.
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto.

1.2 Redes inalámbricas.

1.2.1 Concepto de red inalámbrica.

Una red de área local inalámbrica o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio o infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales, cable UTP, fibra óptica, etcétera., que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, etcétera.) como se aprecia en la Figura 1.9.

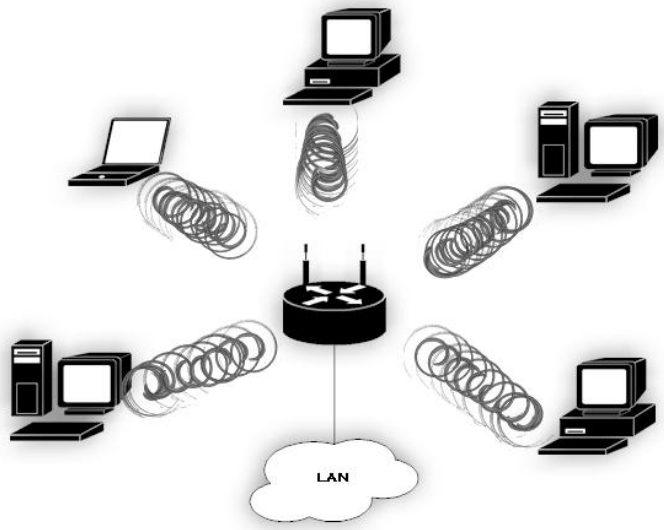


Figura 1.9 Red inalámbrica.

Las redes locales inalámbricas más que una sustitución de las LAN's convencionales son una extensión de las mismas, ya que permiten el intercambio de información entre los distintos medios en una forma transparente al usuario.

En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de infraestructura, enlazando los diferentes equipos y móviles asociados a la red.

Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 10 y los 100 Mbps frente a los 10, 100 y hasta 1000 Mbps ofrecidos por una red de cableado estructurado.

Las redes inalámbricas, además de permitir extender las redes LAN existentes en las organizaciones, son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite o

cuando el tiempo por el cual se requiere contar con una red LAN es corto. En general las WLAN se utilizarán como complemento de las redes de cableado estructurado.

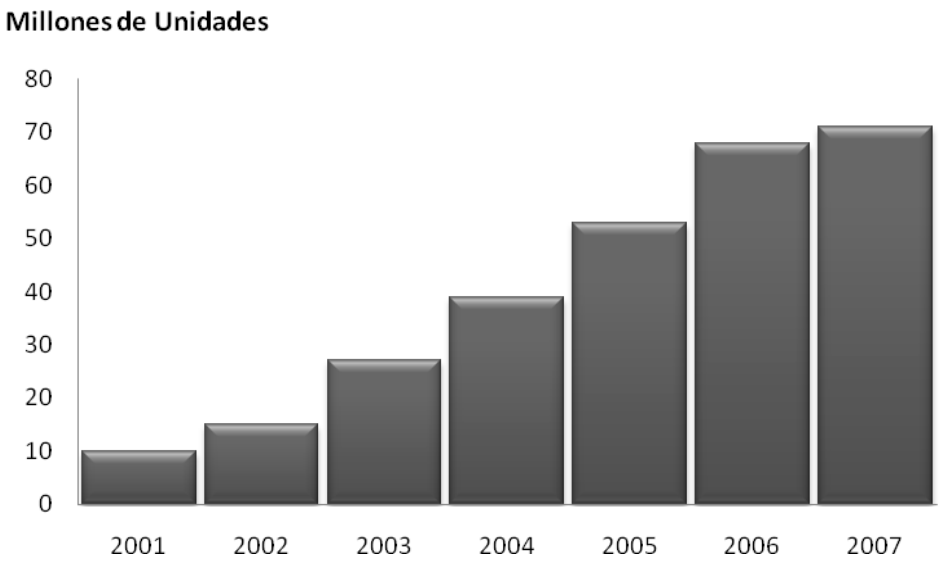
1.2.2 Orígenes.

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

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 la FCC (Federal Communications Comission) de Estados Unidos de América (EUA) asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro disperso.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria, ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

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



Fuente: In StatMDR www.instat.com

Figura 1.10 Crecimiento del mercado.

Sin embargo (ver Figura 1.10), se viene produciendo estos últimos años un crecimiento explosivo en este mercado. Y esto es debido a distintas razones:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles.

- La conclusión de la norma IEEE 802.11 para redes de área local inalámbricas que ha establecido un punto de referencia y ha mejorado en muchos aspectos estas redes.

1.3 Aplicaciones.

Las aplicaciones más típicas de las WLAN que podemos encontrar actualmente son las siguientes:

- En edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.

- Donde se requiere reconfigurar la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

- En redes locales para situaciones de emergencia o congestión de la red cableada.

- En hospitales, fábricas, almacenes y cualquier sitio donde el usuario requiera tener acceso a la información mientras el usuario se encuentra en movimiento.

- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada, ya que la solución inalámbrica es más viable para un plazo corto de tiempo.

- En ambientes industriales con severas condiciones ambientales, este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

- Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de áreas locales cableadas situadas en dos edificios distintos.

1.4 Ventajas y desventajas de las redes inalámbricas.

En la tabla 1.2 se muestran las ventajas y desventajas tanto de las redes inalámbricas como de las redes de cableado estructurado.

Tabla 1.2 Ventajas y desventajas redes inalámbricas.

	Cableado estructurado	Redes inalámbricas
Ventajas.	• Tecnología madura. • Altas velocidades de transmisión. • Confiabilidad. • Cumple con estándares de la industria.	• Buenas características de desempeño. • Resistencia a las interferencias externas. • Seguridad física. • Facilidad de instalación. • Facilidad de mantenimiento. • Facilidad de detección de fallos. • Imprescindible en ciertas circunstancias geográficas. • Menor tiempo de instalación. • Buen nivel de integración con redes tradicionales existentes. • Mínima capacidad para la instalación y el soporte.

Desventajas.	• Reparaciones costosas. • El tiempo de reparación es mayor. • Dificultad para el tendido del cableado o la reutilización de éste. • Mayor tiempo de instalación.	• Potencia y distancias limitadas. • Velocidad de transmisión limitada. • Alto costo por unidad. • Es una tecnología relativamente nueva.

1.5 Access Point.

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Muchos WAP pueden conectarse entre sí para formar una red aún mayor. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Los AP siempre están a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada (Figura 1.11).

Un único AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

Figura 1.11 Access Point.

1.6 Antenas.

Una antena es un conductor de longitud definida que se coloca al final de la línea de transmisión, y que se encarga de transmitir al ambiente, o irradiar, la señal suministrada por el equipo. La antena posee el comportamiento menos predecible, esto debido a que interacciona fuertemente con todo lo que lo rodea y solo se puede saber su comportamiento real hasta que se pone a prueba.

1.6.1 El radiador isotrópico.

El radiador isotrópico es una antena perfectamente omnidireccional, con cero decibeles de ganancia, que irradia la señal en forma de esfera perfectamente uniforme, con la misma intensidad en todas las direcciones (Figura 1.12). Ésta es una antena imaginaria, que no puede fabricarse porque cualquier antena, sin importar qué tan perfectamente esté construida, tiene una ganancia dada en alguna dirección. Esa ganancia puede ser de tan solo unas fracciones de dB, pero ahí está presente siempre.

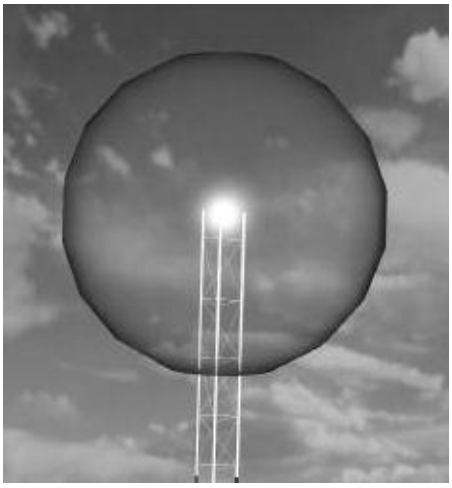


Figura 1.12 Radiador isotrópico.

La ganancia de una antena es una medida de su tendencia a concentrar la señal en una dirección específica. Una antena con alta ganancia es altamente direccional, mientras que una antena con baja ganancia es omnidireccional. La unidad para medir la ganancia es el decibel (dB). El decibel, en antenas, es una relación logarítmica entre voltajes, que se utiliza principalmente para medir ganancia, esta puede ser positiva o negativa.

También podemos dar la medida en dBd. Si hablamos de 10 dBd estamos diciendo que la antena posee 10 dB de ganancia más que el dipolo ideal. O sea, poniendo ambas antenas lado a lado, el dipolo ideal daría una ganancia de 2.15 dB, mientras que nuestra antena daría 10 dB más, o sea, 12.15 dB.

Para convertir de dBi a dBd (y viceversa) se emplea la siguiente fórmula:

$$dBi = dBd-2.15$$

En el mercado es común ver ganancias expresadas en dBi, principalmente por el efecto de "impacto" que tiene el ver un número más grande. Para un fabricante que busca vender antenas resulta muy cómodo el dBi, pero para un comprador que quiere saber cómo se

comporta una antena tiene poca utilidad porque se compara la antena a una antena no existente, que nunca ha existido y de cuyo funcionamiento no se tiene mayor idea. Para nosotros lo mejor sería expresar la ganancia en dBd, dando una idea más realista de su funcionamiento.

1.6.2 Patrón de irradiación de una antena.

Cada antena tiene su propia forma de irradiar una señal. Hay antenas que irradian más en una dirección que en otra, hay otras que tienden a irradiar casi por igual en todas las direcciones, y hay antenas que irradian sólo en ciertas direcciones.

La forma característica que tiene una antena de emitir la señal es lo que se conoce como su patrón de irradiación.

En un patrón de irradiación hay direcciones en las que se emite mucha energía, y direcciones en donde no se emite energía del todo, a estas se les conocen como direcciones "sordas" de las antenas, en donde prácticamente no se reciben señales.

Los patrones de irradiación de una antena por lo general son brindados por el fabricante en las especificaciones.

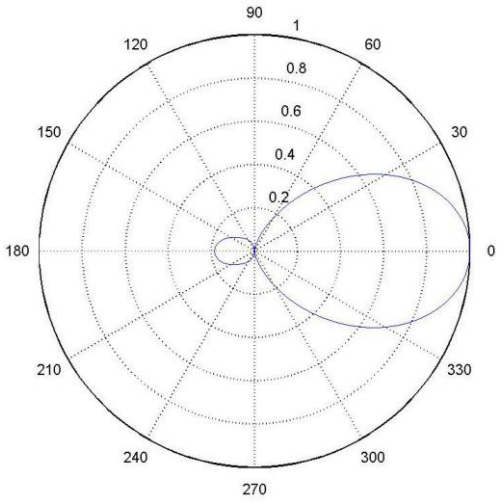


Figura 1.13 Patrón Azimutal.

En la Figura. 1.13 se muestra el llamado patrón azimutal, que sería la forma de irradiar de la antena si se estuviera observando desde arriba. Los puntos donde la curva (la elipse) se aleja más del centro del gráfico son las direcciones que tienen mayor ganancia, mientras que los puntos donde la curva toca el centro son direcciones de cero irradiación.

Dependiendo de la zona a la que se le quiera ofrecer el servicio es la antena que se debe escoger por ejemplo, las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores. Las antenas sectoriales se suelen utilizan cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa (Figura 1.14).

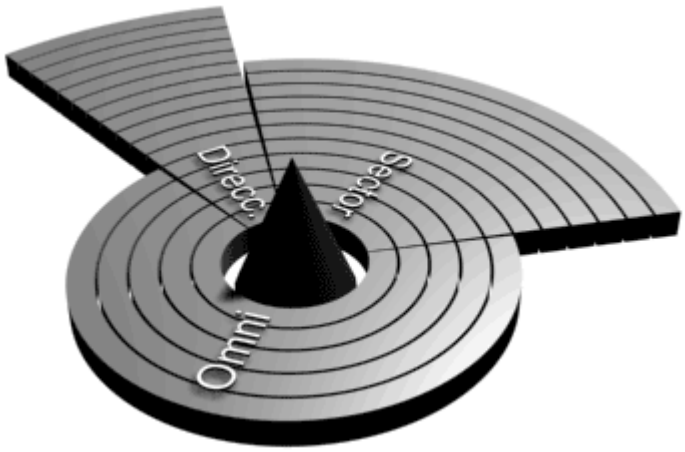


Figura 1.14 Zona de cobertura en los tipos de antenas.

1.6.3 Impedancia, frecuencia resonante.

Existen dos características importantes de una antena que se deben tener presentes en todo momento, las cuales son su frecuencia resonante y su impedancia.

1.6.3.1 Frecuencia resonante.

Es la frecuencia a la cual la antena se vuelve eléctricamente resonante, y en la cual existe una cancelación interna mínima de la señal de radio. A esta frecuencia resonante la antena irradia el 100% de la señal que se le proporciona.

1.6.3.2 Impedancia.

La impedancia de una antena es una especie de resistencia que posee toda antena, y de hecho todo sistema eléctrico, y que se deriva del efecto combinado de resistencia de los elementos, reactancias capacitivas y reactancias inductivas. La impedancia afecta la transferencia de energía entre las diferentes partes de un sistema de radio. En cuanto a impedancia, la regla general es que para lograr una máxima transferencia de energía a la antena, la impedancia de la antena debe ser igual a la impedancia de la línea de transmisión, la cual debe ser igual a la impedancia del equipo de radio.

1.6.4 Tipos de antenas.

Existen muchos tipos diferentes de antenas disponibles en el mercado. Cada antena tiene sus características propias de funcionamiento y sus requerimientos en cuanto a altura, alimentación, etcétera.

Una antena que irradia básicamente por igual en todas direcciones se llama antena omnidireccional. La antena que concentra la señal hacia una dirección específica se llama antena direccional.

1.6.4.1 Antenas de Sector.

Al igual que las antenas omnidireccionales, su uso es para conexiones punto a multipunto. Éstas, sin embargo, sólo emiten en una dirección Su radio de cobertura está entre los 60 y los 180 grados (figura 1.15). La ganancia de estas antenas es mejor que las omnidireccionales (aproximadamente 22 dBi), y permiten orientarlas hacia la dirección que mas interesa (incluso hacia arriba y hacia abajo).

Figura 1.15 Antena de sector.

1.6.4.2 Antenas de Panel.

Se utilizan para conexiones punto a punto enfocadas. Son como pequeñas cajas planas y tienen una ganancia de hasta 22 dBi (figura 1.16).

Figura 1.16 Antena de panel.

1.6.4.3 Antenas Yagi.

Las antenas yagi, (o direccionales) tienen forma de tubo. En su interior tienen unas barras de metal que cruzan el interior de ese tubo. La señal que emiten es direccional y proporciona una ganancia que oscila entre los 15 y los 21 dBi. Hay que enfocarla directamente al lugar con el que se quiere enlazar (figura 1.17).

Figura 1.17 Antena Yagi.

1.6.4.4 Antenas Parabólicas.

Las antenas parabólicas son las más potentes que se pueden adquirir (hasta 27 dBi), por lo que son las más indicadas para cubrir largas distancias entre emisor y receptor. Cuanta mayor ganancia tienen, mayor diámetro de rejilla (figura 1.18).

Figura 1.18 Antena Parabólica.

1.6.4.5 Antenas Dipolo.

Este tipo de antenas, están más indicadas para lugares pequeños, y más concretamente para uso de Access Points. La ganancia de esas antenas oscila entre los 2 y los 5 dBi (figura 1.19).

Figura 1.19 Antena dipolo.

1.7 Estándares y protocolos de las redes inalámbricas.

El estándar 802.11 es un estándar de protocolo de comunicaciones que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

El estándar 802.11 fue desarrollado por el instituto de Ingenieros Eléctricos y Electrónicos (IEEE), para las redes inalámbricas.

1.7.1 Protocolos.

- *802.11 legacy.*

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la

banda 2.4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

- *802.11b.*

La revisión 802.11b del estándar original fue ratificada en 1999. El protocolo 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

- *802.11a.*

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. El protocolo 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede ínter

operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso, esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

- *802.11h.*

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

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU (Intenational Telecommunication Union) que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares.

Con el fin de respetar estos requerimientos, el estándar 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

- *802.11g.*

En Junio de 2003, se ratificó un tercer estándar de modulación el 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

- *802.11n.*

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar

varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado).

- *802.11e.*

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

  - (EDCA) Enhanced Distributed Channel Access.
  - (HCCA) Controlled Access.

- *802.11i.*

Esta dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado).

- *802.11 Super G (protocolo propietario).*

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz, alcanza una velocidad de transferencia de 108 Mbps. Esto es proporcionado por el chipset Atheros.

1.8 Canales y frecuencias.

- IEEE 802.11 b.

Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11b 22-MHz-de-par-a-par (tabla 1.3).

Tabla 1.3 Canal y frecuencia IEEE 802.11b para 22 Mhz.

		Dominios Reguladores				
Id del Canal	Frecuencia en MHz	América	EMEA	Israel	China	Japón
1	2412	X	X		X	X
2	2417	X	X		X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X		X	X
11	2462	X	X		X	X
12	2467		X			X
13	2472		X			X
14	2484					X

- IEEE 802.11a

Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11a 20-MHz-de-par-a-par (tabla 1.4).

Tabla 1.4 Canal y frecuencia IEEE 802.11a para 20 MHz.

		Dominios Reguladores			
Id del canal	Frecuencia en MHz	América	EMEA	Israel	Japón
34	5170		X		
36	5180	X		X	
38	5190		X		
40	5200	X		X	
42	5210		X		
44	5220	X		X	
46	5230		X		
48	5240	X		X	
52	5260	X			X
56	5280	X			X
60	5300	X			X
64	5320	X			X
149	5745				
153	5765				
157	5785				
161	5805				

1.9 Tipo de redes inalámbricas.

- *Wireless WAN (Wide Area Network).*

Una WAN es una red de computadores que abarca una área geográfica relativamente extensa, típicamente permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red.

Por medio de una WAN Inalámbrica se pueden conectar las diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

En sí la forma más común de implantación de una red WAN es por medio de Satélites, los cuales enlazan una o mas estaciones bases, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites utilizan una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35,784 Km.

Por el advenimiento de nuevas tecnologías celulares como 2.5G y 3G, se podría predecir, que el nacimiento de nuevas redes WAN basadas en PDA’s y teléfonos celulares está por venir. Comunidades de usuarios con intereses comunes, instituciones y empresas, se verán beneficiadas por la conectividad que ofrecerán las redes celulares de datos de la próxima

generación.

Nuevos productos, servicios, y actividades derivadas de estas tecnologías impulsarán cambios radicales en la manera en que se trabaja hoy en día, nuevos negocios basados en estas tecnologías saldrán al mercado, y se verá de una vez por todas las utilidades de tener Internet en cualquier lugar en cualquier momento.

- LMDS.

LMDS (Local Multipoint Distribution Service) es una tecnología inalámbrica vía radio para comunicación entre puntos fijos. El rango de frecuencias utilizado varia entre 2 y 40 GHz dependiendo de la regulación del país en el que se utilice.

LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 Km. Las antenas de los receptores se sitúan generalmente en los tejados de los edificios para procurar una visibilidad directa con el transmisor central.

Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes.

- WiMAX.

WiMAX (Worlwide Interoperability for Microwave Access) es una organización sin ánimo de lucro creada en abril de 2002 por fabricantes y suministradores de equipos inalámbricos. El objetivo de WiMAX es promover el uso de las tecnologías IEEE 802.16ª la cual permite crear redes inalámbricas metropolitanas de banda ancha.

Desde el punto de vista de la cobertura una estación base típica WiMAX tiene un alcance de hasta 50 Km. Aunque la cobertura típica suele ser

menor 10 Km. Por otro lado desde el punto de vista del servicio una estación base puede ofrecer servicio a más de 60 empresas (a 2 Mbps) y cientos de hogares (a 256 Kbps) simultáneamente.

- *Wireless LAN (Local Area Nework).*

La Wireless LAN permite conectar una red de computadores en una localidad geográfica, de manera inalámbrica para compartir archivos, servicios, impresoras, y otros recursos. Usualmente utilizan señales de radio, las cuales son captadas por PC-Cards, o tarjetas PCMCIA conectadas a laptops, o a slots PCI para PCMCIA de PCs de escritorio. Estas redes en general, soportan tasas de transmisión entre los 11Mbps y 54Mbps (mega bits por segundo) y tienen un rango de entre 30 a 300 metros, con señales capaces de atravesar paredes.

Estas tecnologías son de gran uso en bibliotecas, unidades móviles como ambulancias para los hospitales, etcétera.

En los Estados Unidos, muchas bibliotecas han implantado con éxito Wireless LAN a costos mucho más bajos de lo que saldría implantar redes físicas, y además les permiten acceso a la red en cualquier lugar de la biblioteca a todos sus usuarios.

- WI-FI.

Wi-Fi (Wireless-Fidelity) es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Fue creado para ser utilizado en redes locales inalámbricas; con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzando distancias de hasta varios cientos de metros. No obstante, versiones mas recientes de esta tecnología permiten alcanzar los 22, 54 y hasta 100 Mbps.

- HomeRF.

En 1998 se creo un grupo de trabajo bajo el nombre HomeRF (Home Radio Frecuency) con el objetivo de desarrollar y promover un sistema de red inalambrica para el hogar a pricipios de 1999 HomeRF saco la version 1.0 de su protocolo SWAP (Shared Wireless Access Protocol) el cual permite transmitir datos a 1.6 Mbps y mantener hasta cuatro comunicaciones duplex de voz. Tiene un alcance de unos 50 metros y una potencia de transmisión de 100mW.

- *Wireless PAN (Personal Area Network).*

Permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información. La líder es esta área es el estándar Bluetooth, una tecnología de radio de corto alcance (2.4 GHz) que simplifica las comunicaciones entre dispositivos de red y otras computadoras. Debido a que no fue diseñada para soportar grandes cargas de tráfico, no es una buena alternativa para sustituir redes locales o amplias.

- Bluetooth.

Bluetooth fue desarrollado en 1994 por la empresa sueca Ericsson con el objetivo de conseguir un sistema de comunicación de los teléfonos móviles con sus accesorios (auriculares, computadoras, etcétera).

Las comunicaciones de Bluetooth se llevan a cabo mediante el modelo maestro/esclavo. Un Terminal maestro puede comunicarse hasta con siete esclavos simultáneamente.

Bluetooth utiliza la técnica FHSS (Frequency Hopping Spread Spectrum, Espectro Expandido por Salto de Frecuencia) en la banda de frecuencias de

2.4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57.6 Kbps en la otra o comunicaciones simétricas de 432.6 Kbps en ambas direcciones. Por otro lado, puede transmitir tanto voz como datos.

- Infrarrojo.

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja.

Los sistemas de comunicaciones de infrarrojo pueden ser divididos en dos categorías:

Infrarrojo de haz directo. Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.

Infrarrojo de haz difuso. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales. Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo coste e inmunes a interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance, el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen interferencias.

IrDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares:

IrDA-Control. Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos.

IrDA-Data. Es un protocolo orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de 1 metro y a velocidades que van desde los 9.6 Kbps hasta los 16 Mbps.

1.10 Topologías.

1.10.1 AD-HOC.

En una topología AD-HOC (Figura.1.20), los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas AD-HOC serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

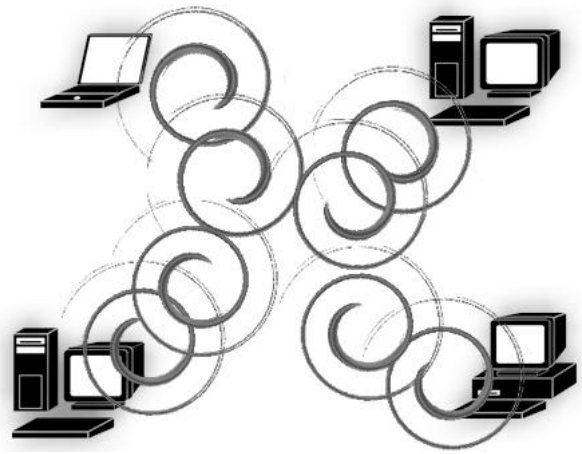


Figura. 1.20 Topología AD-HOC.

1.10.2 Infraestructura.

Una topología de infraestructura (Figura. 1.20) es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

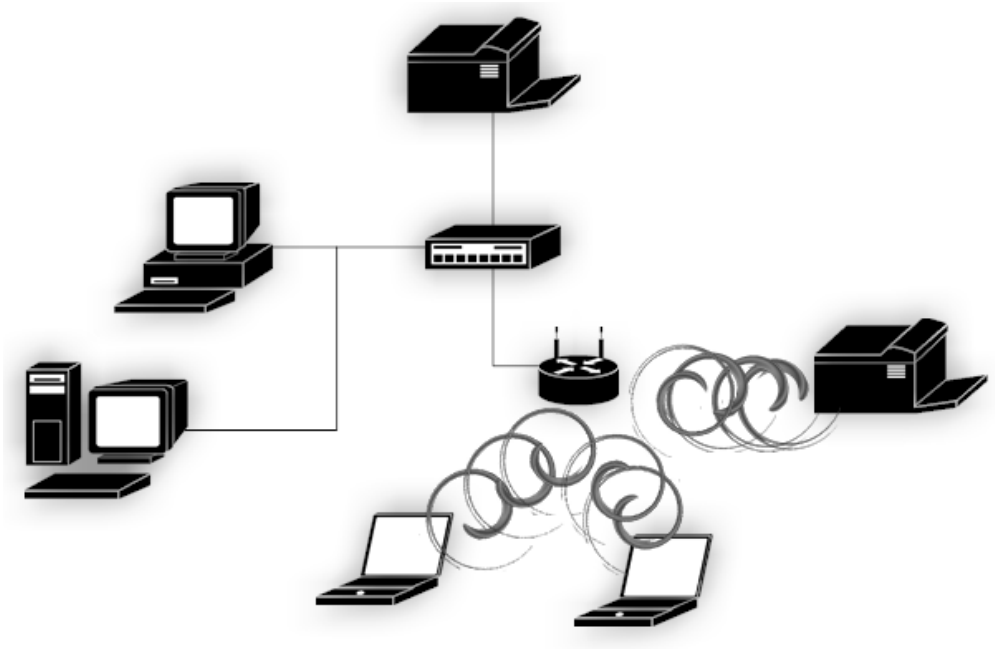


Figura. 1.21 Topología infraestructura.

1.11 Tipos de encriptación para punto de acceso en redes inalámbricas.

La función de la encriptación en un punto de acceso, es la de poder administrar quien puede conectarse a este punto acceso y poder utilizar los recursos de la red inalámbrica, así como la de mantener privados los datos que consultan nuestros usuarios.

1.11.1 WEP (**Wired *Equivalent Privacy).***

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación *IV*) o de 128 bits (104 bits más 24 bits del IV).

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de verificación de integridad CRC.

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo.

El principal problema con la implementación de este algoritmo es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para descifrarlo.

Para atacar una red Wireless se suelen utilizar los llamados Packet sniffers y los *WEP Crackers*. Para llevar a cabo este ataque, se captura una cantidad de paquetes necesaria (dependerá del número de bits de cifrado) mediante la utilización de un Packet sniffer y luego mediante un WEP cracker o key cracker se trata de “romper” el cifrado de la red.

Un key cracker es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Crackear una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.

1.11.2 WPA (*Wi-Fi Protected Access).*

Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP. El método de encriptación WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. El método de encriptación WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida ([PSK] - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

Dos de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Autenticación de los usuarios mediante EAP (Extensible Authentication Protocol), Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. El método WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

1.11.3 WPA2.

Está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

El estándar 802.11i fue ratificado en Junio de 2004.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de EUA - FIPS140-2. El método WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.