UNIDAD 2: RECURSOS DE TECNOLOGIA DE INFORMACIÓN – Infraestructura

Comunicaciones. Redes: Telecomunicaciones y la conectividad de redes. Nuevas tecnologías.

REDES INFORMATICAS

INTRODUCCION

Debido a las computadoras, la gente produce más información que nunca. Esta situación ha creado la necesidad de transferir rápidamente de un lugar a otro, grandes cantidades de datos que, normalmente, son generados por los propios sistemas de computación.

La tecnología relacionada con la comunicación de datos permite a las computadoras y a sus usuarios "hablar" en redes de datos. Esta situación afecta a los sistemas de administración y control de la información de las organizaciones, en especial en lo que hace a la confidencialidad y seguridad de los datos.

Hasta hace un tiempo la posibilidad de que dos computadoras distantes una de otra cientos o miles de kilómetros se conectaran era solo posible para organizaciones muy grandes, las que podían hacer frente a los costos que implicaba. En la actualidad, el desarrollo tecnológico y la disminución de costos en las comunicaciones de datos permiten que cualquier empresa pueda pensar en esta posibilidad.

Hoy se habla de bancos con sus sucursales conectadas a bases de datos centralizadas, permitiendo la transferencia de fondos entre lugares remotos al instante; de cadenas de supermercados que actualizan los precios de los artículos en todos sus locales en forma simultánea con los archivos de sus oficinas centrales; de empresas que disponen de sucursales y que pueden trabajar con datos únicos y centralizados.

Por ejemplo, un caso típico de ambiente informático basado en tecnologías de comunicación de datos se presenta en los sistemas de tarjetas de crédito. El sistema que administra la tarjeta permite actualizar en forma inmediata los consumos realizados por cada socio en negocios remotos y los comerciantes reciben información permanentemente actualizada respecto a tarjetas habilitadas o inhabilitadas, autorización de compras, y cualquier información que deba ser conocida por los comercios que integran el sistema.

En general los sistemas informáticos que utilizan comunicación de datos se caracterizan por trabajar con **información en tiempo real** (los datos de sus archivos son actualizados en el mismo instante en que se producen los eventos modificatorios de la información vigente hasta ese instante) y no podrían funcionar sin contar con un servicio de comunicación de datos que vincule las computadoras que intervienen en las transacciones.

Comunicación de datos

Un sistema de comunicación de datos involucra a varios elementos, necesarios para permitir la transferencia de información de una computadora a otra. Sistemas de comunicación de datos son computadoras interconectadas, cuyos procesadores y terminales no coinciden en situación geográfica, pero cuyos datos fluyen entre ellos a través de algún sistema de telecomunicación.

Mediante los sistemas de telecomunicaciones (usado como sinónimo de comunicación de datos), se puede trabajar en el hogar y transmitir los resultados de la labor diaria electrónicamente a una oficina distante; recabar información financiera para vender o adquirir acciones dentro de la red de la Bolsa; enviar y recibir correo electrónico, buscar una bibliografía y recibir una lista de artículos, libros y documentos seleccionados dentro de una base de datos computarizada localizada en otro continente.

En un concepto amplio, comunicación de datos se produce aún dentro de la misma CPU, ya que entre la memoria, la unidad de control y la unidad aritmético - lógica se transfieren datos. Pero el concepto de comunicación de datos - en su acepción más aceptada - abarca sólo a los aspectos relacionados con el intercambio de datos entre varias computadoras, o entre una computadora central y sus periféricos remotos, por ejemplo: pantallas e impresoras, entendiendo por remotos aquellos dispositivos localizados fuera de un ámbito local inmediato.

Los expertos en informática - cuando hablan de "comunicaciones" relacionan computadoras y dispositivos localizados en lugares remotos, conectados entre sí por medio de algún canal: líneas telefónicas u otros más sofisticados como satélites, cables coaxiles, fibra óptica o radio frecuencia, formando redes de datos donde cada nodo integrante de la misma puede recibir información como un simple usuario o brindar datos como un servidor de base de datos.

La necesidad de comunicación de datos se da aún en situaciones mucho más comunes y corrientes, como cuando es imprescindible conectar las cinco computadoras personales que posee un pequeño comercio distribuidas dentro de su salón de ventas, la oficina de administración y el depósito; o conectar un nuevo puesto de trabajo situado en una sucursal o depósito lejano a la computadora central de la empresa.

Sin embargo, para establecer un enlace, los sistemas de comunicación de datos demandan ciertos requisitos para conectar dos computadoras: cada una debe convenir el formato de transmisión según el cual se transmitirán los datos, la velocidad de transmisión, la dirección en que éstos serán enviados, y por último, hacer todas las operaciones de acuerdo con las reglas comunes (protocolo) que gobernarán la transferencia de información.

ELEMENTOS DE UN SISTEMA DE COMUNICACIÓN

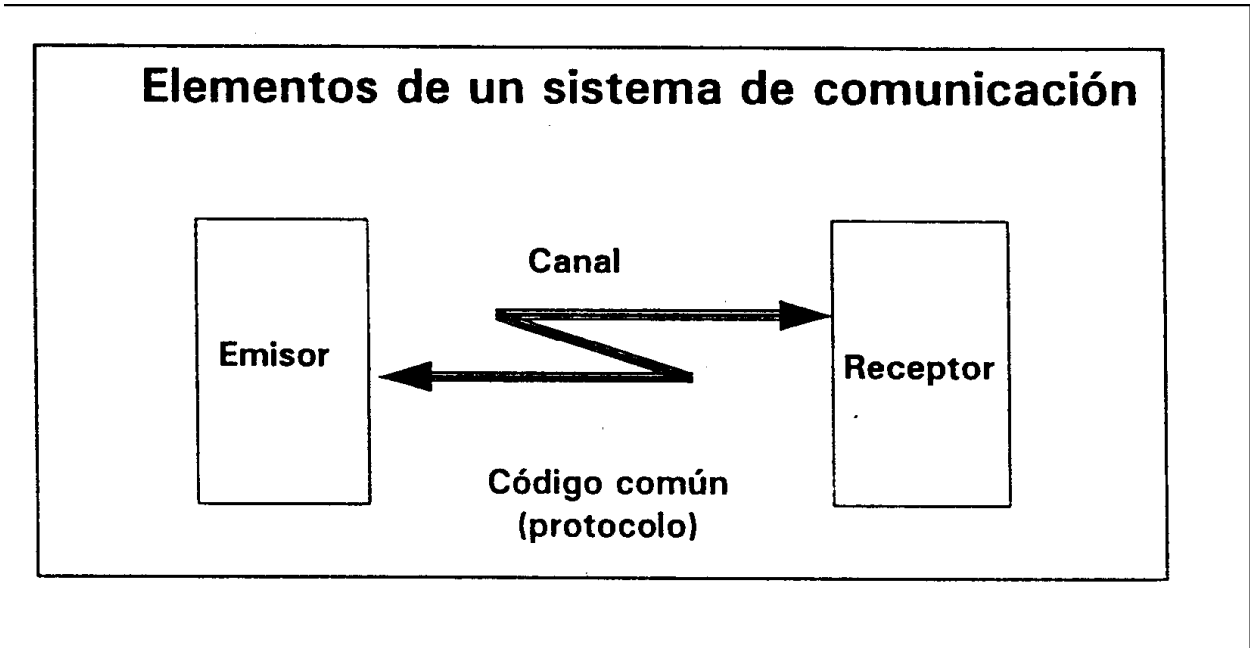
Cualquier comunicación - tanto humana como entre computadoras- para ser establecida necesita cuatro elementos básicos:

- un ente emisor,
- un ente receptor,
- un canal a través del cual se transmite la información,
- un código común para interpretar los datos transmitidos entre ambos entes llamado protocolo en el ambiente de comunicación de datos.

Veamos gráficamente la interrelación de estos cuatro elementos:

Canales para la comunicación de datos

Los canales son los medios físicos por donde fluyen los datos que se transmiten entre las computadoras.



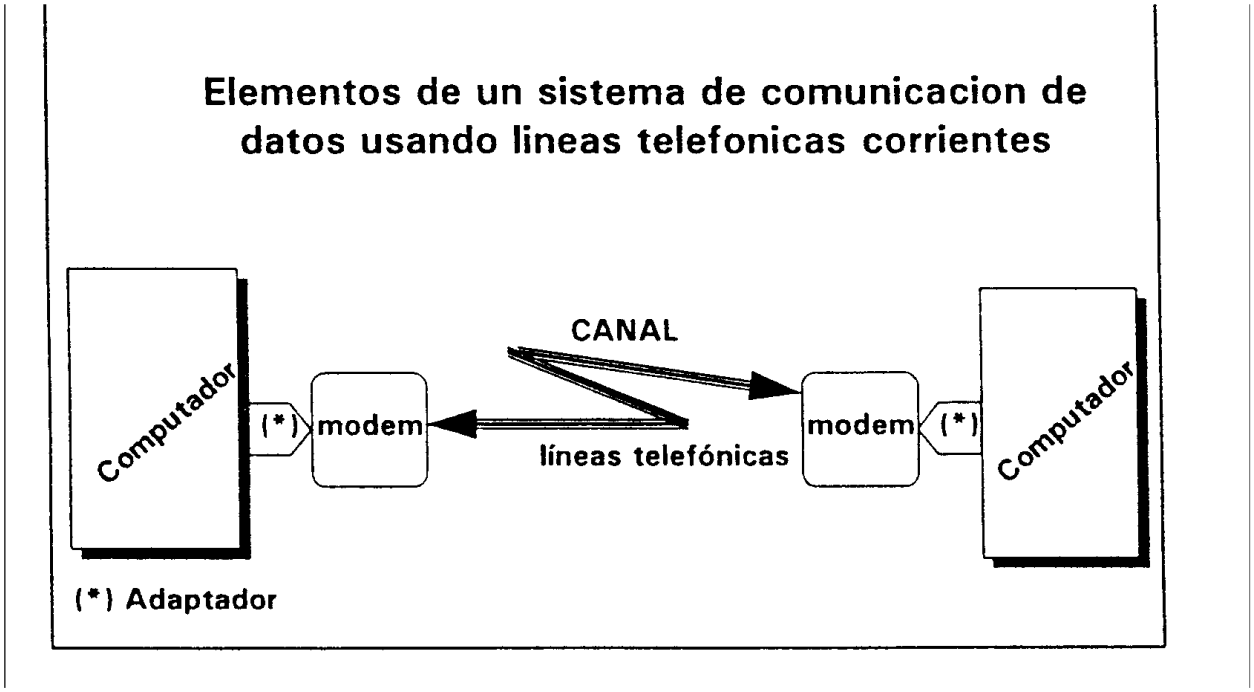
Normalmente las empresas seleccionan un canal de comunicación de datos en base a su velocidad, su costo y la confiabilidad que brindan. A los fines de presentación didáctica, vamos a clasificar los canales para comunicación de datos disponibles actualmente en dos categorías, según la distancia que soportan:

- Canales para ambientes locales: aquellos que soportan las conexiones de computadoras dentro de un edificio en un radio que no pasa los 1000 metros. Tecnologías disponibles: pares trenzados, cable coaxil, fibra óptica, infrarrojo, hondas de luz, etc.

- Canales para distancias largas: aquellos que soportan las conexiones entre computadoras situadas entre distintos edificios, ciudades, países, continentes. Tecnologías disponibles: cables telefónicos, microondas, satélite, fibra óptica, radio frecuencia, etc.

Cuando se comunican computadoras, además de los elementos básicos nombrados, se necesitan de otros dispositivos especiales cuya función principal es adaptar el sistema de codificación interno de la computadora a los canales de comunicación existentes. En la siguiente figura vemos los elementos necesarios para establecer una comunicación de datos cuando utilizamos como canal de transmisión cables telefónicos convencionales:

Elementos de un sistema de comunicación de datos usando líneas telefónicas corrientes



Analicemos cuál es la función que cumplen los nuevos elementos que aparecen en la figura anterior:

Adaptador

Este dispositivo provee la adaptación del flujo de datos que sale de la computadora (o las terminales) con los equipos de comunicación de datos. Las funciones específicas realizadas por los adaptadores pueden ser variadas, pero todos ellos cumplen al menos con las siguientes:

- Adaptar las diferencias de velocidad existente en el flujo de datos que sale del procesador con la velocidad del equipo de comunicación.
- Convertir el flujo de salida de datos de la computadora, de paralelo a serie, y de serie a paralelo cuando el flujo de datos entra.

Tipo y velocidad de transmisión

Los datos pueden ser comunicados por métodos de transmisión en serie o en paralelo. Las computadoras, cuando transmiten sobre las líneas de teléfono, lo hacen generalmente en el modo serial.
La transmisión en serie envía la información de un bit a la vez. La velocidad de transmisión en serie se mide en bits por segundo (bps).

La transmisión en paralelo envía los 8 bits que se necesitan para representar un carácter (1 byte) cada vez. Requiere por lo menos de una conexión con ocho conductores (hilos), uno para cada bit. Es el modo de comunicación típico para conectar los dispositivos locales (dentro del mismo ambiente donde está el procesador).

La velocidad de transmisión se mide en caracteres por segundo (cps). Usualmente la transmisión en paralelo es más rápida que la transmisión en serie. Normalmente la transmisión en paralelo está limitada a pocos metros de distancia, de modo que sólo es posible para transmisiones entre una computadora y sus periféricos conectados en forma local, tales como unidades de disco, impresoras, cintas magnéticas, etc.

Módem

Los datos pueden ser transmitidos en forma analógica (por onda continua) como ocurre en el sistema telefónico o en forma digital como trabaja la computadora.

Las computadoras procesan datos en código binario y tal código es transmitido en señales digitales, que son alternaciones entre dos estados o niveles bien definidos de tensión eléctrica: la presencia (1) o la ausencia (0) de voltaje. En contraste, los teléfonos manejan y transmiten ondas de sonido, que son señales analógicas. Por consiguiente en la transmisión de datos a través de líneas telefónicas, la información almacenada en la computadora debe ser convertida del formato digital a formato analógico. Esta función la cumple el **modem.**

Las señales recibidas (de la computadora) por un módem en forma digital son convertidas a señales analógicas para que puedan ser transmitidas por la línea telefónica; esta operación se denomina modulación. El proceso inverso, convertir señales analógicas en digitales, se denomina demodulación. Como dijimos, el dispositivo que realiza esta tarea se denomina módem (abreviatura de **mo**dulation-**dem**odulation).

Para los PC, los módem pueden ser internos o externos. Un módem interno es una plaqueta de circuitos que se instala en una ranura *(slot)* de expansión de una computadora personal de arquitectura estándar. Un módem externo es un dispositivo separado que se conecta a una interfaz serial ó USB de un PC. La interfaz serial más común es la RS-232.

Los módem generalmente vienen con el software necesario para su operación básica; por ejemplo, contemplan las actividades de marcado automático de teléfono y contestación automática de llamadas. Así, un módem puede marcar automáticamente números telefónicos a los que están conectadas otras computadoras.

Los módems corrientes ofrecen velocidades de transmisión que varian entre 14.400 bps a 56.000 bps y más. El precio del módem aumenta en función de la velocidad que ofrece. Los negocios de hoy requieren de módems más rápidos y eficientes para agilizar las comunicaciones, ahorrando así tiempo y dinero en llamadas telefónicas de larga distancia. Pero existe un límite práctico en la cantidad de *baudios* (cantidad de bits transmitidos por segundo) de un módem, pues está en función del ancho de banda de la línea de comunicaciones, que dicta la máxima velocidad de transmisión.

Antes de concluir con el tema de dispositivos relacionados con comunicación de datos, es necesario destacar que existen también otros elementos especiales utilizados para establecer sesiones de comunicación de datos. Estos resultan imprescindibles para comunicar computadoras en ambientes de red; por ejemplo tenemos a los ruteadores (routers), multiplexores, Hubs, convertidores de protocolo (PAD), puentes (bridges), switch y otros.

El control de la comunicación (protocolo)

Cuando hay dos personas o más comunicándose, deben observarse ciertas reglas para que se produzca un intercambio de información significativa. De la misma manera, para las comunicaciones entre computadoras se requiere respetar reglas destinadas a administrar el flujo de información. Por ejemplo, los elementos de una disciplina de comunicaciones entre personas pueden considerar alguno de los siguientes aspectos:

- ¿Se ha establecido contacto con la persona correcta?
- Sólo una persona puede hablar a la vez
- Se debe hablar en un mismo idioma
- Las porciones de conversación no claras se deben repetir
- En cierto punto, ambas partes se despiden y termina la conversación.

De la misma manera, los elementos de una disciplina o protocolo de comunicación entre computadoras deben considerar aspectos tales como:

- Códigos de lenguajes.
- Formatos de lenguajes.
- Métodos de detección de errores.
- Métodos de corrección de errores.
- Procedimientos para establecer la conexión.
- Procedimientos de terminación y desconexión de la sesión.
- Procedimientos de transferencia de mensajes.
- Modo de transmisión.

La comunicación entre el emisor y el receptor en un sistema integrado por computadoras se realiza mediante la transmisión de datos a través de un camino que los une. Este camino puede ser físico o lógico. El camino es físico cuando las computadoras están unidas directamente por un cable u otro canal que las une (en este caso coinciden el camino lógico con el físico). El camino es lógico cuando se unen a través de una red donde los datos llegan de una computadora a otra a través de distintos caminos físicos.

Por el camino "viajan" conjuntos finitos de bits denominados **paquetes** de datos. Las características del camino a recorrer impondrán en cada caso las reglas para estructurar la información; sin embargo, debe considerarse que es más sencillo comunicar computadoras donde los caminos físicos y lógicos coinciden. A continuación veamos algunos aspectos relacionados con dicha estructuración:

- **Identificación del camino:** La comunicación de dos computadoras en una red se realiza mediante un "diálogo" instrumentado por paquetes de datos que viajan por distintos caminos físicos; para que los mensajes lleguen a destino, se requiere que cada paquete identifique las direcciones de las computadoras (direcciones de destino y de origen o remitente del mensaje).
- **Codificación del tipo de mensaje:** Para establecer una sesión de comunicación, deben enviarse -además de los paquetes que contienen los datos "útiles"- otros tipos de paquetes: de inicio y terminación de la sesión, de confirmación de recepción, de re-envio de datos, etc. Para facilitar la interpretación del contenido, cada paquete transmitido tiene asociado un código que identifica su tipo.
- **Detección de errores:** Integrado por los métodos destinados a solucionar los errores de transmisión.

Otra definición de protocolo es la siguiente: conjunto de reglas que regulan el intercambio de información. Un protocolo regulará la forma en que deberán generarse e interpretarse los paquetes de datos enviados o recibidos. Está orientado al control de errores y a la forma de recuperar los datos recibidos erróneamente, a la identificación del camino lógico y a la selección del tipo de mensaje a transmitir. Es decir, dentro de cada mensaje o paquete, además de los datos (objeto final de la transmisión), existirá otra información destinada a permitir: la detección de errores, la identificación del camino, el control del flujo de la información y la identificación del tipo de mensaje de que se trate.

REDES DE COMUNICACION DE DATOS

Las posibilidades de comunicación entre computadoras no están restringidas a dos máquinas a la vez. El intercambio de datos y la necesidad de compartir información dentro de una organización, exige que la comunicación de datos deba ser extendida a muchas computadoras dispersas geográficamente, de distintos modelos, tipos y capacidades, formando lo que se ha dado en llamar "redes de computadoras" enlazadas en un ambiente dé comunicación de datos.

Normalmente es muy difícil definir con exactitud qué es una red de computadoras, ya que es un concepto confuso. En un principio parece ser algo físico: cables que se tienen desde agujeros recién abiertos en las paredes, o que cuelgan de las placas del techo por encima de la cafetera. A continuación la red parece ser software: abundan menúes, sistemas de correo electrónico y programas especiales. La red también genera cambios en la forma de trabajar: un administrador de red pasa a controlar el acceso a nuestros programas, archivos y directorios, nos habilita las claves para acceder al sistema, a los recursos de impresión, etc.

En realidad una red de computadoras es la combinación de elementos de hardware y de software. El hardware está compuesto por los cables y placas de interfase que conectan a las computadoras y terminales con la red. El software controla el acceso a los archivos y programas y administra el sistema de comunicaciones. Quizá la definición más clara de una red es: sistema de comunicaciones que permite

comunicar a los usuarios y compartir los recursos (archivos y periféricos) de las computadoras que la integran. El sistema telefónico es en este sentido un sistema similar a una red de computadoras, ya que en su esencia es un sistema de comunicaciones. Cuando utilizamos un teléfono, pensamos pocas veces en los cables y demás elementos físicos de que está compuesto; en su lugar nos fijamos en el resultado: el establecimiento de una comunicación útil y productiva.

La tecnología vinculada con redes informáticas representan en la actualidad uno de los sectores de mayor importancia dentro del mercado de computación. Agotada la etapa de difusión de las computadoras personales (PC), hoy presentes en todos los sectores de la vida productiva, profesional y personal, la siguiente etapa parece basarse en la necesidad de integración, formando entornos únicos de procesamiento de datos dentro de la empresa, dentro del mercado, en el mundo (como ocurre con Internet).

CLASIFICACIÓN DE LAS REDES

Se denomina red de computadores una serie de host (terminales) autónomos y dispositivos especiales intercomunicados entre sí. Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de las mismas, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

Las posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

Clasificación de las redes según su tamaño y extensión:

1. **Redes LAN.** Las redes de área local (Local Área Network) son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).

2. **Redes MAN.** Las redes de área metropolitana (Metropolitan Área Network) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.

3. **Redes WAN.** Las redes de área amplia (Wide Área Network) tienen un tamaño superior a una MAN, y consisten en una colección de host o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un router a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros.

4. **Redes Internet.** La Internet es una red de redes, vinculadas mediante ruteadores y gateways. Un gateway o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10000 kilómetros en adelante, y su ejemplo más claro es Internet, la red de redes mundial.

5. **Redes inalámbricas.** Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Clasificación de las redes según la tecnología de transmisión:

a. **Redes de Broadcast.** Aquellas redes en las que la transmisión de datos se realiza por un solo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.
b. **Redes Point-To-Point.** Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos routers.

Clasificación de las redes según el tipo de transferencia de datos que soportan:

I. **Redes de transmisión simple.** Son aquellas redes en las que los datos sólo pueden viajar en un sentido.
II. **Redes Half-Duplex.** Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.
III. **Redes Full-Duplex.** Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

NOTA: Se considera como nodos remotos a los dispositivos situados a una distancia superior a los 300 metros (a veces se habla de 1.000 metros), distancia a partir de la cual es necesario agregar dispositivos especiales para permitir la transmisión de datos. Entendemos por nodo a las computadoras, terminales, impresoras, y cualquier otro dispositivo con capacidad de procesamiento conectado en forma directa a una red de comunicación de datos.

En los primeros tiempos de la computación, todos los datos de la empresa *y* los propios de cada departamento eran gestionados en un sector especializado: el área de Sistemas o Centro de Cómputos. Este departamento se ocupaba en forma exclusiva de brindar los servicios informáticos de toda la empresa. Cada usuario se conectaba al sistema principal por medio de terminales no inteligentes o "bobas", caracterizadas por ser incapaces de realizar ningún proceso en forma autónoma. La computadora central era la encargada de realizar todo el procesamiento de los datos de la organización, aunque esto pudiera sobrecargarlo en algunas ocasiones. Este modelo, hoy cuestionado, configura el modo de procesamiento centralizado.

A medida que las computadoras personales se fueron haciendo más poderosas con el uso de procesadores más avanzados y de software más sofisticado, los usuarios de los sistemas basados en grandes computadoras (mainframes) comenzaron a romper con sus costumbres y con las de sus departamentos de sistemas. Comenzó a ser patente que las computadoras personales podían ofrecer un modo más efectivo de producir informes y de mantener la información que se necesita a nivel de departamento.

La primera ruptura con los sistemas tradicionales y su jerarquía comenzó a principios de los 70, cuando algunas minicomputadoras comenzaron a sustituir a los grandes sistemas *mainframes* en algunos sectores del mercado. Estos sistemas eran lo suficientemente baratos para que se distribuyeran en distintos departamentos dentro de una sola empresa. Estos a su vez podían estar ligados por distintos métodos de comunicaciones, formando los primeros sistemas de proceso distribuido.

Por lo que el siguiente paso fue ligar entre si los nuevos centros de procesamiento de datos basados en minicomputadores, formando los primeros sistemas de procesamiento distribuido y las primeras redes LAN y WAN. Con esta nueva arquitectura de procesamiento los administradores de cada departamento podían gestionar ahora sus propios recursos informáticos y tener acceso a otros resultados del procesamiento de sus datos que los proporcionados hasta entonces por el Centro de Cómputos.

En los entornos centralizados, con grandes computadoras, el procesador y la memoria son recursos únicos dentro del sistema. Hay varias razones para tener una única computadora: menores costos de adquisición y de mantenimiento, mayor seguridad de los datos y facilidad de gestión. En las arquitecturas de procesamiento distribuidas, basadas en redes, la mayor parte de los procesos se lleva a cabo en la memoria individual de las computadoras que integran la red, denominadas estaciones de trabajo o workstation. El servidor de archivos o Server reemplaza la función del gran equipo central, y generalmente, es una PC común de uso especializado en la administración de los archivos de datos centrales de la empresa.

Con el avance de las telecomunicaciones, en nuestros días estamos ante un nuevo punto de inflexión de la tecnología informática. Internet e intranet están revolucionando la forma en que se tratan los datos dentro y fuera de la organización. Hoy se presentan como la evolución de los conceptos que relacionaban y diferenciaban las redes LAN y WAN.

REDES DE AREA LOCAL (LAN)

Las redes de área local o LAN (Local Área Network) se han convertido en la arquitectura de equipamiento de mayor difusión dentro de la industria informática, amenazando reemplazar en el corto plazo a la arquitectura tradicional y centralizada, representada por los tradicionales grandes computadoras *(mainframes)*

Las redes LAN se caracterizan por estar confinadas a un ambiente de reducidas distancias entre los nodos, usualmente dentro de un edificio y con un radio de operación que suele tener como límite máximo los 300 metros (distancia que varía según la tecnología disponible y las características de los nodos a conectar).

Las redes LAN, además de permitir compartir recursos de hardware, solucionan la anarquía en los sistemas de información de las empresas producida por sistemas informáticos instrumentados en computadoras aislados. Permiten integrar soluciones informáticas encaradas sectorialmente por los departamentos de la empresa en Un único sistema de información global.

Los nodos de los sistemas LAN enlazan dispositivos categorizados según las funciones que prestan: servidores de datos, estaciones de trabajo y periféricos de uso público. Las redes LAN permiten la transmisión de datos entre las computadoras conectadas a la misma, proporcionan servicios tales como: administración de archivos, impresión de trabajos, comunicación entre los nodos y correo electrónico.

La característica distintiva de una red local es el uso de estaciones de trabajo inteligentes, esto supone un alto grado de procesamiento distribuido, asignado a las computadoras personales de, los usuarios. A diferencia de las grandes computadoras, que conectan terminales “tontos” a procesadores centrales, las redes locales permiten a los PC de uso individual mantener y usar su propia capacidad de cálculo.

Una LAN puede ser un sistema cerrado que utiliza sus propios métodos de comunicación, lo que significa que otros fabricantes no pueden integrar sus productos a la misma. Una red también puede ser un sistema abierto, esto ocurre cuando se ofrece a otros fabricantes las especificaciones para incluir “ligaduras” de programación que les permitan crear con facilidad aplicaciones complementarias. Un sistema abierto se ajusta a un conjunto de reglas y métodos que se convierten en un estándar de la industria. La estandarización permite que distintos proveedores diseñen productos que interaccionen fácilmente con los productos de otros fabricantes.

Tipos de redes LAN

Según las características del sistema operativo que las administra existen varios tipos de redes LAN, a los efectos de una presentación didáctica los agrupamos en:

Sistemas punto-a-punto

En una red punto a punto, cualquiera de sus estaciones puede funcionar como un servidor que ofrece sus recursos a las restantes estaciones de trabajo. Las PC pueden ser sólo receptoras, cuando acceden a los recursos de otras estaciones sin compartir las suyas propias.

Las redes punto-a-punto pueden parecer el sistema ideal a primera vista, pero carecen de facilidades para mantener una adecuada seguridad y velocidad de comunicaciones.
Aunque este Sistema fue el canalizador para establecer los primeros estándares de LAN en el ámbito industrial, actualmente no es la mejor plataforma para construir una red como lo exige la tecnología vigente (de alta velocidad, segura y eficiente) Como ejemplos de **sistemas operativos** para redes punto-a-punto tenemos a: *Lantastic,* el paquete de Novell para pequeñas redes (de 2 a 5 usuarios); *Windows 9X*.

Sistemas con servidor no dedicado

Una LAN con servidor no dedicado es aquella que asigna a una estación de trabajo de la red las funciones de servidor de archivos. Es decir, la computadora que contiene el sistema operativo de la red (que administra la LAN), es a la vez estación de trabajo y servidor de archivos; el servidor se convierte así en dos máquinas. Aunque parece ideal, esta situación normalmente disminuye la eficiencia global de la red, ya que la LAN tiene como servidor de archivos a una computadora que debe compartir sus recursos entre las peticiones individuales realizadas por la estación de trabajo y las grupales efectuadas por las otras PC de la red.

Como ejemplos de sistemas operativos con servidor no dedicado, tenemos a: *Netware 2.2,* un producto ya descontinuado de Novell para pequeñas redes (de 5 a 20 usuarios); *Windows NT,* la versión de Microsoft para grandes redes; etc.

Sistemas con servidor dedicado

Este ambiente es el más difundido actualmente en las redes LAN, caracterizándose por tener una computadora asignada exclusivamente como servidor de archivos. Un servidor dedicado es aquel que no puede ejecutar directamente programas de los usuarios, dado que funciona como un dispositivo que administra los archivos de datos comunes, atendiendo las peticiones de las estaciones de trabajo y gestionando los datos requeridos por los programas de los usuarios.

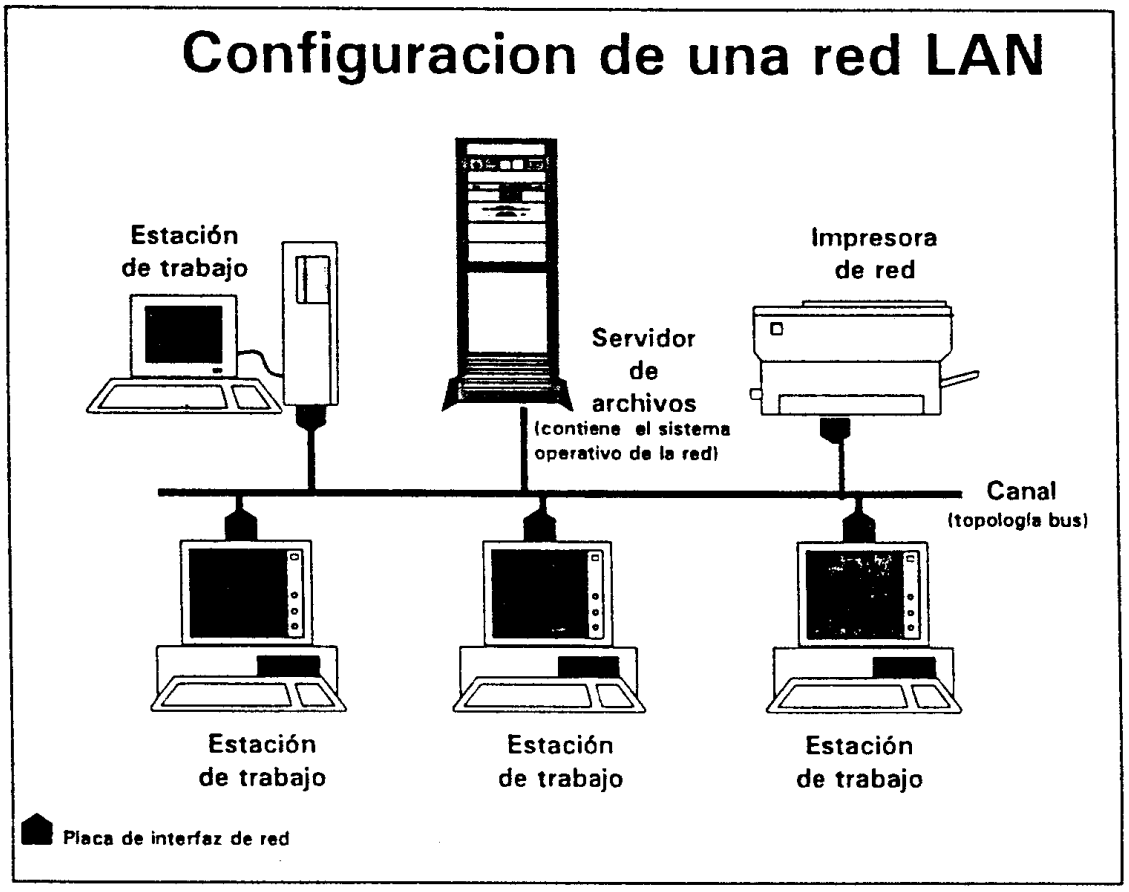
En estos sistemas los discos fijos del servidor son administrados por el sistema operativo de la red y reciben un formato especial, más adecuado en lo que hace a seguridad y velocidad de acceso. En síntesis, los sistemas LAN con servidor dedicado ofrecen mejores respuestas en lo que hace a velocidad de comunicaciones, seguridad de acceso y administración de recursos. Como ejemplos de sistemas operativos con servidor dedicado tenemos a: *Netware,* el paquete de Novell para grandes redes (de 5 a 100 usuarios); *LAN Manager,* la solución de IBM para integrar PC; etc.

Ventajas de las redes LAN

Originalmente, una de las razones para instalar redes de área local fue el compartir recursos caros, como discos, impresoras etc. Ahora este aspecto de las redes se ha hecho menos importante al haber bajado el precio de los periféricos y han aparecido otras razones más importantes en apoyo del uso de redes de área local, tales como la disponibilidad de un amplio abanico de productos de software multiusuario que se ajusta a las necesidades de la empresa, argumento que quizá puede ser la mejor razón para instalar una red local; otras razones valederas y que justifican instalar una LAN, pueden ser las siguientes:

- **Trabajo en común:** Conectar un conjunto de computadoras personales formando una red, permite que un grupo o equipo de personas involucrados en proyectos comunes pueda comunicarse más fácilmente y compartir programas o archivos de un mismo proyecto.
- **Actualización y mantenimiento del software:** Si el software se almacena en forma centralizada en un servidor, es mucho más fácil actualizarlo en todas las computadoras de la empresa. En lugar de tener que actualizarlo individuamente en cada uno de los PC de los usuarios, el administrador tendrá que actualizar la única copia almacenada en el servidor.
- **Copia de seguridad:** La administración de las copias de seguridad de los archivos de la empresa son más simples, ya que los datos están centralizados.
- **Facilidad de organización:** Los miembros de un grupo de trabajo ya no necesitan trabajar más en ubicaciones contiguas para poder compartir sus archivos e información con otros miembros del grupo; la red provee el medio para transferir los datos comunes que necesitan.
- **Uso compartido de impresoras y otros periféricos:** El uso compartido de los recursos siempre ha sido una de las grandes ventajas y argumento para justificar la instalación de las redes de área locales; si bien algunos periféricos son lo suficientemente baratos como para situar uno por cada puesto de trabajo, otros permanecen a un precio que obliga compartirlos en la red, por ejemplo, las impresoras láser, los plotters, etc.
- **Correo electrónico:** Un buen sistema de correo electrónico *(e-mail)* permite que los usuarios se comuniquen fácilmente entre sí. A cada usuario se le asigna un "buzón electrónico" para recibir su correo en el servidor; los otros usuarios dejan sus mensajes en el buzón electrónico correspondiente al destinatario y éste los lee cuando accede a la red. Hoy, con el fenómeno de Internet, este argumento es uno de los más importantes para justificar la instalación de una LAN dentro de una organización.

Elementos para configurar una LAN



Los elementos a los que hacemos referencia a continuación corresponden a las redes de área local más difundidas, como las administradas por los sistemas operativos *Netware* de Novell, *Windows NT* de Microsoft o *Lan Manager* de IBM. Los componentes físicos y de software que detallamos son considerados los elementos necesarios y suficientes para formar una red de área local, ellos son: servidor de archivos, estaciones de trabajo, placas de interfaz, cableado de la red y sistema operativo.

Los ilustramos en la siguiente figura:

a) Servidor de archivos

El servidor de archivos de una red LAN está representado por una computadora dedicada a gestionar el sistema de archivos comunes de la misma. El servidor, además de controlar las comunicaciones de la red, suele realizar Otras funciones como: dar servicio a las impresoras del sistema, mantener las seguridades de acceso, los usuarios autorizados, etc.

Como vimos, un servidor de archivos puede estar dedicado en cuyo caso emplea toda su potencia de procesamiento para las funciones de administración de la red; o puede ser no dedicado en este caso emplea parte de sus recursos para atender procesos propios de una estación de trabajo, y la parte restante de su potencia de procesamiento la asigna para administrar la red.

El sistema operativo de la red está cargado (grabado) en los discos fijos del servidor de archivos junto con las herramientas necesarias para la administración de la red y los programas de aplicación del usuario. Cada vez que se enciende la red, el sistema operativo se carga y el servidor queda bajo su control. La seguridad del sistema emana del hecho de que las unidades de disco fijo de la red sólo pueden ser activadas o accedidas después de arrancar el sistema operativo de la red, residente en el servidor de

archivos. Así los subsistemas de seguridad de la LAN se encargan de controlar e impedir el acceso al sistema por parte de personas no autorizadas.

La elección de las características técnicas para un equipo que será usado como servidor de archivos es crítica y es determinante del rendimiento y funcionamiento eficiente de una LAN. La tarea principal de un servidor de archivos es procesar las peticiones realizadas por cada una de las estaciones de trabajo de la red. Estas peticiones pueden ser: acceso a disco, a colas de impresión o comunicarse con otros dispositivos. La recepción, gestión y ejecución de estas peticiones puede requerir un tiempo considerable, tiempo que se incrementa en forma proporcional al número de estaciones de trabajo activas en la red. Como el servidor gestiona las peticiones de todas las estaciones de trabajo, su carga puede ser muy pesada.

Si las estaciones de trabajo envían peticiones de forma continua y masiva, se puede llegar a un estado de congestión permanente. El tráfico de la red puede llegar a ser tan elevado que podría impedir la recepción de algunas peticiones enviadas por las estaciones de trabajo. Estas seguirían enviando peticiones adicionales hasta obtener respuesta por parte del servidor, lo que incrementa aún más la carga de trabajo del servidor de archivos, ya que tiene que procesar también las peticiones adicionales. En situaciones de congestión, también se ve afectado el rendimiento de una estación de trabajo al tener que esperar respuestas a los pedidos enviados al servidor para continuar con su tarea.

Cuanto mayor es el número de usuarios que tiene una red, resulta más importante disponer de un servidor de archivos con elevadas prestaciones. Necesita estar configurado con una memoria RAM de gran tamaño para optimizar los accesos a disco y mantener las colas de impresión. El rendimiento de un servidor de archivos es una combinación de varios factores: tipo y velocidad del procesador, el tamaño de los canales de acceso a memoria y disco, el tamaño del *bus,* la existencia de memoria *cache,* las velocidades de acceso y transferencia del disco fijo y su controlador, las prestaciones de las placas de comunicaciones (placas de interfaz de la red), etc.

b) Estaciones de trabajo

Las estaciones de trabajo se conectan al servidor a través de una placa de conexión de red (placa de interfaz de red - NIC) y el cableado correspondiente. Las estaciones de trabajo para las LAN, en general, deben ser sistemas con capacidad de procesamiento propia como las computadoras personales (PC). Las terminales no-inteligentes utilizadas en los ambientes de grandes computadoras y minicomputadoras no pueden utilizarse en las redes LAN, ya que no poseen capacidad propia de procesamiento.

Los sistemas LAN trabajan con el concepto de procesamiento distribuido, esto es, las computadoras (estaciones de trabajo) conectadas a la red utilizan su propia capacidad de procesamiento para cargar y ejecutar los programas del usuario y toman los datos desde el servidor de archivos. Esto libera al servidor para que pueda especializarse en tareas de administración de la red. Efectuado el procesamiento en la estación de trabajo, los datos de los archivos son actualizados en el servidor, desde donde pueden ser compartidos por otras estaciones de trabajo.

Una PC debe satisfacer un reducido conjunto de requisitos para ser utilizada como estación de trabajo. De hecho un microcomputador con una configuración básica puede, servir, siempre que pueda arrancar correctamente (desde el disco fijo, un disquete o de la placa de red cuando ésta posee un sistema de inicialización remota o *boot ROM).* A diferencia de los terminales no inteligentes utilizados en sistemas centralizados multiusuario, las estaciones de trabajo de una red se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sean los elementos con que se configuran, mejor.

La difusión de virus informáticos en los ambientes de procesamiento donde existen PC, justifica la conveniencia de utilizar estaciones de trabajo sin disqueteras. Al carecer de disqueteres, no existe la posibilidad de copiar archivos confidenciales en disquetes y sacarlos de la empresa, ni traer programas extraños.

c) Placas de interfaz de red

Las placas de conexión de red permiten enlazar a las computadoras de la red (servidores y estaciones de trabajo) al canal de comunicaciones de la misma. En la práctica el canal es representado por un cable.

En primer lugar, la placa de red provee el conector físico, necesario para conectar el cable de la red a la computadora. También incluye los programas *(drivers)* - dentro de sus circuitos internos- que suministran el protocolo de enlace con las órdenes necesarias para comunicar la computadora con la red a la que debe integrarse.

d) Cableado de la red (Canal)

Una vez que contamos con las estaciones de trabajo, el servidor de archivos y las placas de red, estamos en condiciones de conectarnos al canal de la red. Con este elemento contamos con todos los dispositivos físicos necesarios para configurar una red LAN.

Los tipos de canales para redes LAN más utilizados son: el par trenzado de tipo telefónico (UTP), el coaxil (BNC) y la fibra óptica. Además, se pueden realizar conexiones por vías menos frecuentes, tales como enlaces a través de radio o microondas. Cada tipo de canal tiene sus ventajas y desventajas; algunos son propensos a interferencias, mientras que otros no son recomendables de usar por razones de seguridad. La velocidad y la longitud del tendido son los principales factores técnicos a considerar en el momento de decidir el tipo de canal a utilizar.

Par trenzado

Este canal de transmisión es de uso común en EEUU (sistema telefónico). También se usa para configurar LAN pequeñas, con velocidades de operación de 1 a 10 Megabits por segundo.

Consiste en dos conductores aislados individualmente trenzados entre sí para disminuir interferencias con otros pares cercanos. Posee un pequeño ancho de banda, lo que limita la transmisión a unos pocos caracteres por segundo.

Ofrece como ventajas su bajo costo y el ser una tecnología bien estudiada (no requiere habilidades especiales para su instalación) y ofrece una buena respuesta (atenuación) frente a interferencias.

Cable Coaxil

Consiste en dos conductores concéntricos, donde el conductor central (de cobre) está recubierto de material aislante; el segundo conductor -malla trenzada metálica de aluminio- envuelve al primero y todo el conjunto va dentro de una vaina protectora aislante.

El cable está disponible en dos espesores: cable grueso diseñado para dar soporte a largas distancias (más caro y difícil de manipular); y cable fino (más barato y práctico de manipular), este último es el utilizado para conectar redes de hasta 300 metros.

El cable coaxil es un canal de alta capacidad utilizado en sistemas de comunicaciones y de video; se usa también para transmitir la señal de TV por cable. A pesar de la similitud de apariencias, existen múltiples tipos de cable coaxil, cada uno diseñado con un diámetro y una impedancia diferentes según el propósito para el cual fue fabricado: señal de TV, banda base, banda ancha, etc.
Características: soportan comunicaciones en banda ancha y en banda base, es útil para transmitir varias señales simultáneamente (voz, vídeo y datos), es fácil de instalar, con velocidades de hasta 10 MBits.

Fibra óptica

Consiste en un núcleo interior de vidrio (con un cierto índice de refracción) que permite el paso de energía luminosa (haces de láser), recubierto a su vez por vidrio (de distinto índice de refracción con respecto al núcleo) que tiene por finalidad guiar las ondas luminosas a través del núcleo y minimizar las pérdidas, estando todo el conjunto protegido con una vaina de material aislante.

Está reemplazando gradualmente a los conductos de cobre y coaxiles, tanto en telefonía como en transmisión de datos.

Comparativamente son menos caros y mucho más eficientes que los cables coaxiles. Un cable coaxil usual puede conducir alrededor de 5000 canales de voz, en tanto que un cable de fibra óptica más delgado conducirá 10 veces esa cantidad. A medida que las compañías telefónicas cambien sus líneas troncales a fibra óptica, sus capacidades de comunicación de datos se incrementarán notablemente.

Ventajas que ofrece la fibra óptica

- Gran ancho de banda, lo que implica una mayor capacidad de información a conducir.
- Alta velocidad de transmisión, (más de 140 Megabits/Seg.)
- Está libre de interferencias electromagnéticas.
- Tiene bajas pérdidas, lo que posibilita tramos más largos entre repetidores y regeneradores de la señal.
- Ofrece una mayor confiabilidad y seguridad, ya que resulta muy difícil de intervenir o adulterar.

Dispositivos de redes

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

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

"Bridges" (Puentes): Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

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

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

Topología de las redes

Relacionado con los canales está la topología o diseño de la red. Se llama topología de red a la forma que asume el diseño de la conexión entre los nodos que integran una red de comunicación de datos. Puede considerarse a la topología como la forma en que se distribuyen los cables de la red para conectar los nodos de la misma.

La topología de una red es importante porque determina dónde pueden colocarse los nodos y cómo se conectarán, es decir determina la facilidad con que se tenderá el cable (canal) y el costo de todo el sistema de comunicaciones. Existen tres topologías básicas: estrella, anillo y bus; aunque en la práctica suelen presentarse como combinaciones o topologías mixtas.

Topología Estrella

En ella cada nodo está conectado a una computadora central. Un nodo de la red puede ser una computadora de cualquier tamaño. La comunicación entre las computadoras conectadas en forma radial debe pasar a través de la computadora central. El diagnóstico de problemas en la red es fácil, debido a que las estaciones de trabajo se comunican a través del equipo central. Los fallos en los nodos son fáciles de detectar y también es fácil cambiar los cables.

Un banco con computadoras en cada sucursal, podría usar topología estrella. Cada sucursal procesa sus transacciones dentro de su nodo local y luego transmite los datos acumulados del día a los archivos maestros de la computadora central en la oficina matriz.

Topología Anillo

Conecta o une a las computadoras en un lazo cerrado. Un mensaje destinado a un nodo específico viaja a través de cada nodo alrededor del anillo hasta alcanzar a su destino. El mayor riesgo de una red en anillo es que si un nodo se vuelve inoperante, toda la red se para.

Con la topología en anillo, las redes pueden extenderse a menudo a largas distancias; el costo total del cableado será menor que en una configuración en estrella. Sin embargo, el complicado cableado debe cerrarse sobre si mismo y una rotura en el cable hará caer todo el sistema.

Topología de bus

Permite conectar diversos nodos (computadoras) con un solo canal (cable), a lo largo del cual las estaciones pueden enviar mensajes en uno y otro sentido. Para enviar un mensaje, una computadora temporalmente toma el control del cable colector o bus y lo transmite.

Cuando usamos la topología bus en una red LAN, el servidor de archivos y todas las estaciones de trabajo están conectados a un cable general central. Todos los nodos comparten este cable y éste necesita contar con dos acopladores (llamados terminadores) en ambos extremos.

El cable puede extenderse de cualquier forma a través de las paredes y techos de la instalación y las estaciones de trabajo. Para conectarse a la red, sólo se pinchan" en el mismo.

Híbridas

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

.

* Anillo en estrella

Esta topología se utiliza con el fin 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.

* "Bus" en estrella

El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

* Estrella jerárquica

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

e) Sistema operativo de la red LAN

Por último, necesitamos el software para administrar la red de área local o el sistema operativo de la LAN; éste normalmente reside en el servidor de archivos y se ocupa básicamente de dos tareas: administrar las comunicaciones entre los nodos que integran la red y administrar los archivos comunes en cuanto a seguridad de acceso y compartir datos en un ambiente multiusuario.

En cuanto al acceso de múltiples usuarios a un mismo dato, el sistema operativo de la LAN "bloquea" los registros que están siendo utilizados por un usuario de modo que impide que otros los usen hasta que dicho usuario haya terminado el proceso y liberado los registros. Tal bloqueo de los registros en uso asegura una correcta actualización de los datos y le garantiza a los siguientes usuarios el acceso a información correcta.

La seguridad es otra función importante asignada al sistema operativo de una LAN. Una empresa que instale una LAN puede agregar, a través del sistema operativo de la misma, una gran variedad de controles de seguridad para acceder a su ambiente. Los controles utilizan contraseñas *(password)* para permitir el acceso a la red sólo a quienes conozcan la clave apropiada y los procedimientos de activación necesarios. Complementariamente existen también atributos de seguridad propios para cada archivo y directorio; éstos pueden establecer si un usuario en particular puede grabar en dicho archivo (agregar, modificar o borrar registros) o simplemente leer datos del mismo. También se le asigna al sistema operativo de una LAN otras funciones: manejo de las colas de impresión *(spooling),* comunicaciones con otras redes, etc.

Los productos y soluciones que actualmente ofrece el mercado para ambientes de redes de área local son muchos. Especialmente competitivo se manifiesta actualmente el segmento correspondiente a los sistemas operativos para administrar las LAN. La batalla más fuerte se ha instalado entre Novell con su producto *Netware* y Microsoft con *Windows NT (2000.)*

Prestaciones requeridas a un sistema operativo para redes LAN

Como vimos, el sistema operativo de una LAN se ocupa de administrar los archivos comunes, comunicar a los usuarios, implementar seguridades para el acceso a los recursos de la red, dar servicios de impresión compartida *(spooling),* y otras tareas más; en este caso y con fines de una presentación didáctica, detallamos las prestaciones básicas requeridas a un sistema operativo para redes LAN agrupadas de la siguiente manera:

- **Servicio de archivos:** Básicamente las redes LAN trabajan con archivos compartidos. Tanto el administrador como los usuarios necesitan tener un buen control sobre la copia, almacenamiento y protección de los archivos almacenados en los servidores de datos.
- **Seguridad:** En las redes se tiende a situar los archivos en lugares centralizados y protegidos (en el servidor de archivos.) Esto puede producir problemas cuando gente curiosa intente ver los archivos de otros usuarios, o un novato borre los datos de un registro. A medida que aumenta el número de usuarios de la red, son más necesarias las medidas de seguridad. Será necesario que el administrador de la red asigne a los usuarios derechos de acceso al sistema y a los archivos adecuados. Una vez que se han establecido las medidas de seguridad, ninguna persona debería poder acceder al servidor de la red o a sus archivos sin la autorización correspondiente.
- **Utilidades de gestión:** Cualquier sistema operativo de red debería ofrecer un conjunto completo de programas utilitarios que faciliten un mejor uso de los recursos disponibles por parte de los usuarios finales y de los administradores de la red. Entre otras, pueden existir órdenes que permitan visualizar la situación de la red o evaluar su rendimiento, es decir disponer de utilitarios de diagnóstico para atender los problemas o posibles problemas de comunicaciones y perfomance.
- **Comunicación entre usuarios:** Una de las grandes prestaciones de las redes consiste en que los usuarios puedan comunicarse entre sí fácilmente y enviarse archivos a través de la red.
- **Colas de impresión:** Las colas de impresión permiten que los usuarios puedan seguir trabajando justo después de pedir la impresión de un archivo. Para guardar los archivos que esperan ser impresos, se utiliza la memoria del sistema, normalmente en el servidor o en el servidor de las impresoras. De esta forma los usuarios pueden seguir trabajando con sus programas. Una buena red habrá de tener un buen sistema de gestión de colas de impresión que permita dar prioridad a algunos trabajos sobre otros, o que permita imprimir con una distribución de tiempo, etc.
- **Conectividad entre redes:** Esta característica del sistema operativo contempla la integración de la red que administro a otras redes LAN o WAN; es deseable que la conexión sea “transparente” (pase desapercibida) para el usuario. Esta facilidad hoy es muy requerida ante el fenómeno de Internet; prácticamente todos los sistemas operativos de LAN están ofreciendo facilidades para integrar su ambiente a la red de redes.

Administración de la red: Definición de la estructura de grupos y usuarios en una LAN.

Una red incluye a diversos usuarios con diferentes derechos, privilegios y responsabilidades.

Básicamente, se pueden establecer dos grandes categorías de usuarios: aquellos que poseen responsabilidades en la supervisión de ciertos servicios, llamados **usuarios supervisores**, y los que solamente limitan su accionar al uso de los diferentes recursos que ofrece la red, llamados **usuarios comunes o normales**.

Dentro de los usuarios supervisores, a su vez, se dividen responsabilidades en la administración de la red.

El usuario ADMIN

Cuando se instala la red, automáticamente se crea un usuario denominado ADMIN, quien será el máximo responsable de la administración del sistema. Este posee derechos ilimitados sobre todos los objetos del árbol de directorios.

Usuarios comunes

Todos los usuarios de la red poseen una serie de propiedades que se establecen al momento de definir a cada uno, y que luego pueden modificarse:
Algunas de estas propiedades son:

- Restricciones de conexión.
- Restricciones de clave de acceso (password)
- Restricciones de tiempo de conexión.
- Login script
- Equivalencias de Seguridad
- Pertenencia a grupos de usuarios
- Derechos sobre archivos.

Por otra parte, para cada usuario se puede especificar un directorio de origen en donde almacenará sus programas y datos. El usuario poseerá todos los derechos sobre ese directorio, pudiendo definir todos los subdirectorios que necesite.

Usuarios supervisores

Cuando el usuario ADMIN configura la estructura del árbol de directorios es común que defina un objeto para cada unidad de la empresa. Y luego, para cada una de esas unidades, se definirá un objeto supervisor.

Sus tareas más habituales son:

- Definición del entorno de seguridad.
- Creación y administración de usuarios y grupos de usuarios.
- Definición de operadores que se encargarán de administra determinados recursos de la red.

Operadores

Los operadores son usuarios especiales que tienen como responsabilidad administrar recursos de la red, como servidores o impresoras. En lo que respecta a estos últimos, se definen solo cuando el volumen de la red y de trabajos a imprimir lo justifica. Ellos son los encargados de manejar las colas de impresión, siendo sus tareas eliminar, modificar y agregar entradas a al cola, así como también cambiar el orden de prioridad en los procesos de impresión.

Grupos de usuarios

En una red se pueden establecer diferentes grupos de usuarios que – por lo general – se definen de acuerdo a la tarea que realizan y las aplicaciones que utiliza cada usuario.

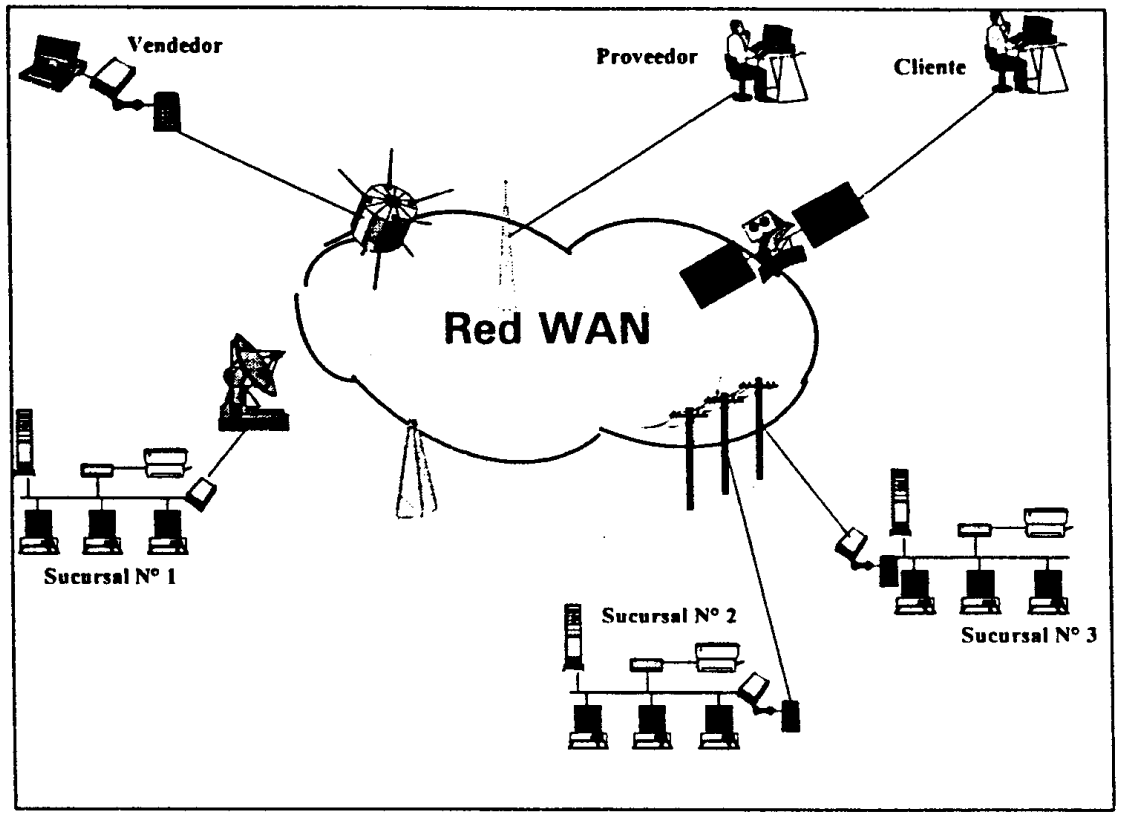
La utilización de grupos de usuarios simplifica la implementación del esquema de seguridad, ya que en lugar de definir los derechos individualmente para cada usuario, se realiza una definición global. Al asignar un usuario a un grupo, este pasa a tener los derechos del grupo sin perder los propios.

Por su parte, cuando se lo da de baja, el usuario no desaparece, sino que simplemente deja de tener los derechos que le correspondían por pertenecer a dicho grupo.

Otra ventaja del trabajo con grupos de usuarios se aprecia en el manejo del correo electrónico. Integrando en grupos de usuarios con intereses comunes se puede – por ejemplo- enviar el correo a todo el grupo. Lo que hará que el mensaje llegue a cada uno de los usuarios pertenecientes a él.

REDES DE AREA AMPLIA (WAN)

Una red de área amplia o WAN *(Wide Area Network)* administra datos y recursos informáticos de computadoras y terminales interconectadas en un ambiente donde las distancias físicas de los nodos trascienden el ámbito de un edificio, exigiendo así usar tecnologías que permitan la comunicación de datos entre lugares remotos. Una red WAN tiene como objetivo brindar servicios similares a los de una LAN; su funcionalidad incluso es similar; difieren en los dispositivos y productos que deben usar para permitir la comunicación de datos entre nodos remotos.



Construir y administrar una WAN puede presentar diversas dificultades: los costos por uso de canales de comunicación para salvar las distancias - usando líneas telefónicas, microondas, satélite u otros medios- pueden elevar exponencialmente el presupuesto del área de sistemas. Es posible crear un red propia usando canales de comunicación "dedicados" (por ejemplo, líneas telefónicas exclusivas), lo que representa mejores prestaciones y costos más elevados en caso de bajo tráfico, o utilizar canales de comunicación compartidos para enlazar los nodos distantes (por ejemplo, líneas telefónicas convencionales o discadas) En ambos casos se requiere además de equipos para la conversión de señales analógicas a digitales y viceversa (módem) y otros dispositivos especiales para comunicación de datos.

La mayoría de los países avanzados han desarrollado en los últimos años "redes públicas digitales", servicio especialmente diseñado para la transmisión de señales digitales. Las redes digitales fueron desarrolladas para la transmisión de datos entre computadoras; superan las limitaciones técnicas de las redes públicas conmutadas existentes actualmente (telefónica y télex) y constituyen el soporte de telecomunicaciones requerido por la telemática. Funcionan bajo protocolo X.25. Algunos ejemplos de redes públicas digitales son: ARPA (primera de este tipo que se puso en funcionamiento en el mundo), TYMNET, TRANSPAC (red pública francesa), DATAPAC (red pública canadiense), IBERPAC (red pública de transmisión de datos de España), etc.

En Argentina, a principios de los '80. Entel instaló la red ARPAC que utiliza tecnología española para redes públicas de datos basada en X.25.

La seguridad también es un problema a resolver en una red WAN. Mientras más nodos tenga un sistema, mayores serán las posibilidades de que usuarios no autorizados obtengan acceso a datos importantes y confidenciales. Por ello se implementan sistemas de protección especiales para el acceso (claves de acceso) y la transmisión de datos (usando "encriptación" de datos).

Como dijimos, las redes digitales son redes WAN de acceso público, donde cualquier usuario que cumpla con los requisitos necesarios (legales y técnicos) puede conectarse a la red de datos. Como contrapartida existen redes WAN de acceso restringido (sistemas cerrados), donde los accesos están vedados al público en general, el sistema de cajeros automáticos BANELCO, la red de reservas aéreas utilizada por Aerolíneas Argentinas, etc.

Otra clasificación corriente de las redes WAN sigue la arquitectura de su diseño, así nos encontramos con:

- **Redes jerárquicas:** En estas redes no son posibles las comunicaciones directas entre los nodos que integran la red, pues todos los mensajes deben pasar por el controlador central de la misma. Como ejemplo tenemos las redes bajo ambiente IBM/SNA, como la red de reservas aéreas.

- **Redes entre iguales**, como ARPAC, INTERNET y otras: consideran a todos sus nodos con la misma jerarquía, independientemente del tamaño y características del dispositivo que se conecta a la red. Así un nodo adherido puede acceder directamente a la computadora de cualquier otro usuario adherido al sistema. Cada nodo tiene un número de acceso a la red, desde el cual poder llamar y ser llamado.

Canales para las redes de área amplia (WAN)

Los módem y las líneas telefónicas son los elementos más difundidos actualmente para conectar computadoras remotas en una red de comunicación de datos. Esta situación continúa vigente a pesar de que las líneas telefónicas regulares son inadecuadas para la transmisión de grandes volúmenes de datos.

Las empresas que diariamente deben transmitir gran cantidad de datos, frecuentemente alquilan líneas dedicadas, especialmente acondicionadas para reducir el ruido típico de las líneas telefónicas y poder transmitir así a mayor velocidad.

La transmisión de datos no siempre requiere conductores o cables en cada paso del camino. Las señales de microondas y ondas cortas, transmitidas entre torres retransmisoras, con frecuencia se emplean como complemento o alternativa a los sistemas de comunicación telefónica. Es corriente que las empresas empleen sistemas de microondas para transmitir datos entre computadoras; el uso de estos canales en algunos casos puede ser más sencillo y más barato que alquilar líneas telefónicas dedicadas.

Otra tecnología que día a día va ganando su espacio en la comunicación de datos en redes WAN es la fibra óptica. Las futuras 'autopistas de información" utilizarán masivamente este elemento como canal troncal. Esta tecnología ya se está usando en el tendido de redes telefónicas para la transmisión de voz.

Por último, debemos considerar otra tecnología reciente para la transmisión de datos a distancia: los satélites. Esta tecnología habilita a los usuarios a enviar datos entre computadoras utilizando los satélites geo-estacionados situados alrededor del mundo. Brindan capacidad de comunicación potencial a computadoras situadas en cualquier lugar de la tierra.

TRANSMISIONES INALÁMBRICAS

Espectro electromagnético

Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar en el espacio libre, aun en el vacío.

La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, f, y se mide en Hz. La distancia entre dos máximos o mínimos consecutivos se llama longitud de onda y se designa con la letra griega λ.

Al conectarse una antena apropiada a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio.

En el vació todas las ondas electromagnéticas viajan a la misma velocidad, sin importar su frecuencia. Esta velocidad, usualmente llamada velocidad de la luz, que es aproximadamente $3x10_8$ m/seg. La siguiente figura muestra el espectro electromagnético. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

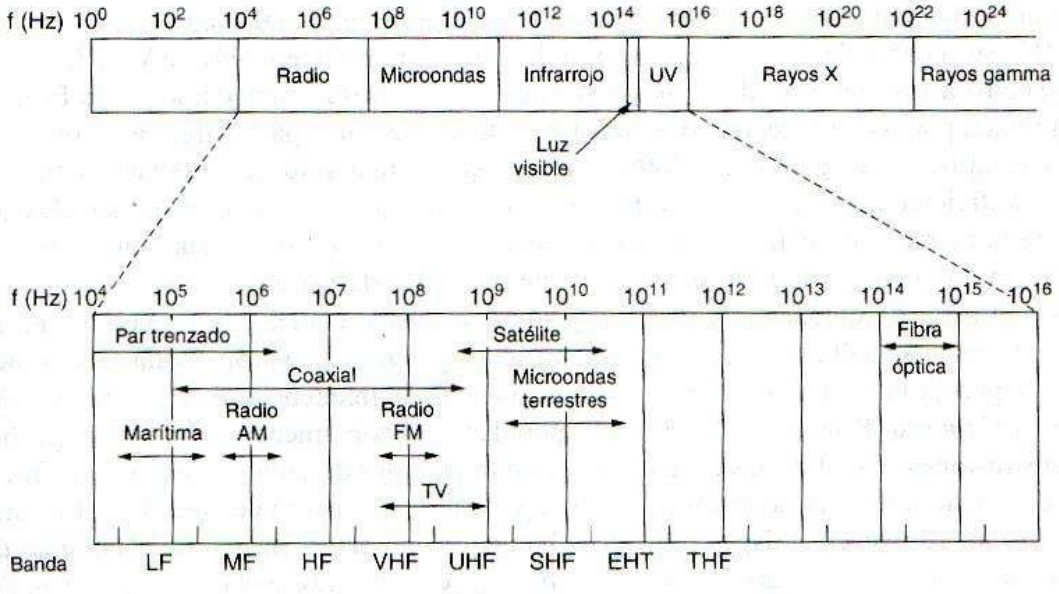


Figura El espectro electromagnético y sus usos para comunicaciones.

Radio Transmisión

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto de interiores como de exteriores. Las ondas de radio también son omnidireccionales, ósea viajan en todas las direcciones desde la fuente, por lo cual el transmisor y el receptor no tienen que alinearse.

Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia.

Todas las ondas de radio están sujetas a interferencia por los motores y equipos eléctricos. Debido a la capacidad de viajar distancias largas y la interferencia entre usuarios, los gobiernos legislan el uso de radiotransmisores.

Transmisión Por Microondas

Por encima de los 100MHZ las ondas viajan en línea recta y, por tanto se pueden enfocar en un haz estrecho. Concentrar toda la energía en haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora se deben alinear entre si.

Ondas Infrarrojas

Las ondas infrarrojas se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja. Estos controles son direccionales, tienen el inconveniente de no atravesar los objetos sólidos.

El hecho de que las ondas infrarrojas no atraviesen los sólidos es una ventaja. Por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio.

Este sistema no necesita de licencia del gobierno para operar en contraste con los sistemas de radio.

Esta propiedad ha hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores.

Transmisión Por Ondas De Luz

Este tipo de transmisión se ha usado durante siglos. Una aplicación es conectar las LAN de dos edificios por medio de láseres montados en la parte mas alta de los edificios, esta señalización óptica es unidireccional por lo que

cada edificio necesita su propio láser y su propio foto detector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. Fácil de instalar y no requiere de licencia.

Por ser un haz muy estrecho tiene ventajas pero también es una debilidad.

La desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, funcionan bien en días soleados.

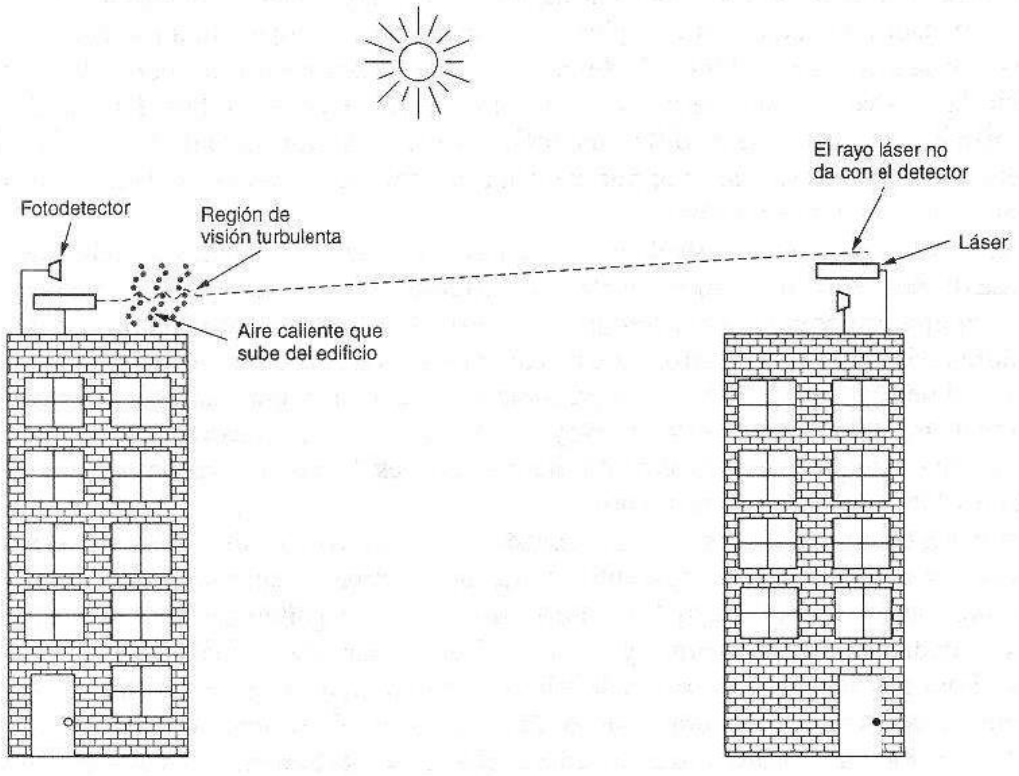


Figura Las corrientes de convección pueden interferir los sistemas de comunicación por láser. Aquí se ilustra un sistema bidireccional con dos láseres.

QUÉ ES UNA WLAN

Introducción

WLAN son las siglas en inglés de Wirless Local Area Network.

Es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta.

Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas. Las WLAN han adquirido importancia en muchos campos incluido el de la medicina.

Ejemplos de uso: ventas al pormenor, almacenes, manufacturación, etc. de modo que se transmite la información en tiempo real a un procesador central.

Cada día se reconocen más este tipo de redes es un amplio número de negocios y se augura una gran extensión de las mismas y altas ganacias.

Por qué utilizar WLAN's

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad. Así mismo la red puede ser más extensa sin tener que mover o instalar cables.

Respecto a la red tradicional la red sin cable ofrece las siguientes ventajas:

- **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.
- **Flexibilidad:** Permite llegar donde el cable no puede.
- **Reducción de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- **Escalabilidad:** El cambio de topología de red es sencillo y trata igual a las redes pequeñas y grandes.

Uso de la redes sin cable en la actualidad

El uso más frecuente de las WLAN es como extensión de la redes cableadas de modo que se da una conexión a un usuario final móvil.

- En hospitales: datos del paciente transmitidos de forma instantánea.
- En pequeños grupos de trabajo que necesiten una puesta en marcha rápida de una red (por ejemplo, grupos de revisión del estado de cuentas).
- En entornos dinámicos: se minimiza la sobrecarga causada por extensiones de redes cableadas, movimientos de éstas u otros cambios instalando red sin cable.
- En centros de formación, universidades, corporaciones, etc., donde se usa red sin cable para tener fácil acceso a la información, intercambiar ésta y aprender.
- En viejos edificios es también más adecuada.
- Los trabajadores de almacenes intercambian información con una base de datos central mediante red sin cable de modo que aumenta la productividad. También para funciones críticas que requieren rapidez.

Tecnología WLAN

Según el diseño requerido se tienen distintas tecnologías aplicables:

 Banda estrecha.
Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

 Banda ancha.
Es el usado por la mayor parte de los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso de no estar en la correcta frecuencia el receptor, la señal aparece como ruido de fondo. Hay dos tipos de tecnología en banda ancha:

a) Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.
b) Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

 Infrarrojos.
No es una técnica muy usada. Se usan frecuencias muy altas para el transporte de datos. Como la luz, los infrarrojos no pueden traspasar objetos opacos. Por lo que o bien se utiliza una comunicación con línea de visión directa o bien es una difusión.

Sistemas directos baratos se utilizan en redes personales de área reducida y ocasionalmente en LAN's específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subrredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales.

Cómo trabajan las WLAN

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponer a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En

una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena. La naturaleza de la conexión sin cable es transparente al sistema del cliente.

Configuraciones de la WLAN

Pueden ser simples o complejas. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual.
Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Figura 1. Red peer-to-peer

Instalando un Punto de Acceso (APs) se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

Figura 2. Cliente y punto de acceso

Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming".

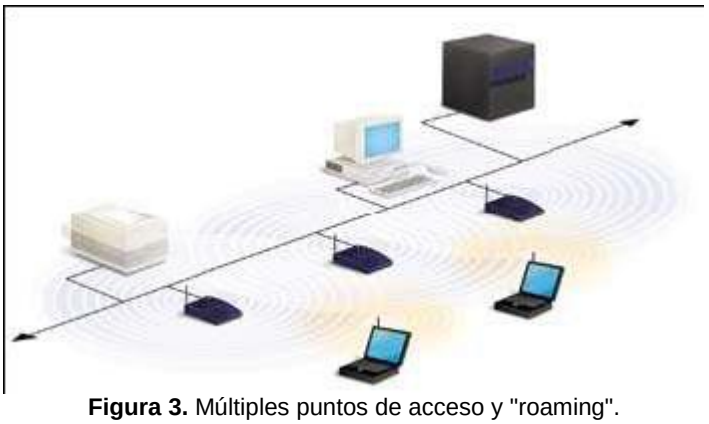


Figura 3. Múltiples puntos de acceso y "roaming".

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

Figura 4. Uso de un punto de extensión.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: se quiere una Lan sin cable a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

Figura 5. Utilización de antenas direccionales.

Sumario

La flexibilidad y movilidad hace de las redes sin cable que sean muy efectivas para extensiones y que sean una atractiva alternativa a las redes cableadas, puesto que proporcionan la misma funcionalidad sin las restricciones del cable en sí mismo. Las redes sin cable permiten topologías desde las más simples hasta complejas redes que ofrecen conexión y distribución de datos y permiten "roaming" (navegar). Además de ofrecer al usuario final movilidad en un entorno de red, habilitan redes portátiles permitiendo a las LAN movimientos con el conocimiento de los trabajadores que las utilizan.

BENEFICIOS DE UNA WLAN

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para enchufar el ordenador, y los administradores de la red pueden poner a punto o aumentar la red sin instalar o mover cables. Veamos más ampliamente sus beneficios.

Visión general de los beneficios de una WLAN

Frente a las redes tradicionales se tienen las siguientes ventajas en cuanto a productividad, comodidad y costos:

- Movilidad: Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- Facilidad de instalación: Evita obras para tirar cable por muros y techos.
- Flexibilidad: Permite llegar donde el cable no puede.
- Reducción de costes: Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- Escalabilidad: El cambio de topología de red es sencillo y trata igual las redes pequeñas y grandes.

WLAN en la industria

- Corporaciones: Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de ficheros, y visualización de web's, independientemente de dónde se encuentren en la oficina.
- Educación: Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con consolas de ordenador conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a internet, etc.
- Finanzas: Mediante un PC portable y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias contables incrementan su productividad con una rápida puesta a punto de una red.
- Cuidado de la salud: WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de transcripción, etc.
- Hotelería y venta al por menor: Los servicios de hotelería pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa. En los almacenes de ventas al por menor una WLAN se puede usar para actualizar temporalmente registros para eventos especiales.
- Manufacturación: WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.
- Almacenes: En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costes del escrutinio de un inventario físico.

QUÉ PRODUCTOS DEBERÍA ADQUIRIR

Son varios los factores a considerar a la hora de comprar un sistema inalámbrico para la instalación de una red Lan. Algunos de los aspectos a tener en cuenta son los siguientes:

Cobertura

La distancia que pueden alcanzar las ondas de Radiofrecuencia (**RF**) o de Infrarojos (**IR**) es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energia. Los objetos sólidos bloquean las señales de infrarrojos, esto impone límites adicionales. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una Lan inalámbrica típica va de 30m. a 100m. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (microcélulas) que permiten "navegar" por la Lan.

Rendimiento

Depende de la puesta a punto de los productos así como del nº de usuarios, de los factores de propagación (cobertura, diversos caminos de propagación), y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red. Para la más comercial de las redes inalámbricas los datos que se tienen hablan de un rango de 1.6 Mbps. Los usuarios de Ethernet o Token Ring no experimentan generalmente gran diferencia en el funcionamiento cuando utilizan una red inalámbrica. Estas proporcionan suficiente rendimiento para las aplicaciones más comunes de una Lan en un puesto de trabajo, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, y acceso a bases de datos y aplicaciones multiusuario. Como punto de comparación una Lan inalámbrica operando a 1.6 Mbps es al menos 30 veces más rápida.

Integridad y fiabilidad

Estas tecnologías para redes inalámbricas se han probado durante más de 50 años en sistemas comerciales y militares. Aunque las interferencias de radio pueden degradar el rendimiento éstas son raras en el lugar de trabajo.

Los robustos diseños de las testeadas tecnologías para Lan inalámbricas y la limitada distancia que recorren las señales, proporciona conexiones que son mucho más robustas que las conexiones de teléfonos móviles y proporcionan integridad de datos de igual manera o mejor que una red cableada.

Compatibilidad con redes existentes

La mayor parte de Lans inalámbricas proporcionan un standard de interconexión con redes cableadas como Ethernet o Token Ring. Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red Lan, aunque con los drivers apropiados. Una vez instalado, la red trata los nodos inalámbricos igual que cualquier otro componente de la red.

Interoperatividad de los dispositivos inalámbricos dentro de la red.

Los consumidores deben ser conscientes de que los sistemas inalámbricos de redes Lan de distintos vendedores pueden no ser compatibles para operar juntos. Tres razones:

- Diferentes tecnologías no interoperarán. Un sistema basado en la tecnología de Frecuencia esperada (FHSS), no comunicará con otro basado en la tecnología de Secuencia directa (DSSS).
- Sistemas que utilizan distinta banda de frecuencias no podrán comunicar aunque utilicen la misma tecnología.
- Aún utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no comunicarán debido a diferencias de implementación de cada fabricante.

Interferencia y Coexistencia

La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede potencialmente dar cierto grado de interferencia en un sistema Lan inalámbrico. Por ejemplo los hornos de microondas, pero la mayor parte de fabricantes diseñan sus productos teniendo en cuenta las interferencias por microondas. Otro problema es la colocación de varias redes inalámbricas en lugares próximos. Mientras unas redes inalámbricas de unos fabricantes interfieren con otras redes inalámbricas, hay otras redes que coexisten sin interferencia. Este asunto debe tratarse directamente con los vendedores del producto.

Licencias

En los Estados Unidos, La Comisión Federal de Comunicaciones (FCC), gobierna la radio-transmisión , incluida la empleada en las redes inalámbricas. Otras naciones tienen sus correspondientes agencias reguladoras. Típicamente las redes inalámbricas se diseñan para operar en porciones del espectro de radio donde el usuario final no necesita una licencia FCC para utilizar las ondas de radio. En los Estados Unidos la mayor parte de las redes difunden en una de las bandas de ISM (de instrumentación, científicas o médicas). Estas incluyen 902-928 Mhz, 2.4-2.483 Ghz, 5.15-5.35 Ghz, y 5.725-5.875 Ghz. Para poder vender productos de sistemas de Lan inalámbricos en un país en particular, el fabricante debe asegurar la certificación por la agencia encargada en ese país.

Simplicidad y Facilidad de Uso

Los usuarios necesitan muy poca información a añadir a la que ya tienen sobre redes Lan en general, para utilizar una Lan inalámbrica. Esto es así porque la naturaleza inalámbrica de la red es transparente al usuario, las aplicaciones trabajan de igual manera que lo hacían en una red cableada, Los productos de una Lan inalámbrica incorporan herramientas de diagnóstico para dirigir los problemas asociados a los elementos inalámbricos del sistema. Sin embargo, los productos están diseñados para que los usuarios rara vez tengan que utilizarlos.

Las Lan inalámbricas simplifican muchos de los problemas de instalación y configuración que atormentan a los que dirigen la red. Ya que únicamente los puntos de acceso de las redes inalámbricas necesitan cable, ya no es necesario llevar cable hasta el usuario final. La falta de cable hace también que los cambios, extensiones y desplazamientos sean operaciones triviales en una red inalámbrica. Finalmente, la naturaleza portable de las redes inalámbricas permite a los encargados de la red preconfigurar ésta y resolver problemas antes de su instalación en un lugar remoto. Una vez configurada la red puede llevarse de un lugar a otro con muy poca o ninguna modificación.

Seguridad en la comunicación

Puesto que la tecnología inalámbrica se ha desarrollado en aplicaciones militares, la seguridad ha sido uno de los criterios de diseño para los dispositivos inalámbricos. Normalmente se suministran elementos de seguridad dentro de la Lan inalámbrica, haciendo que estas sean más seguras que la mayor parte de redes cableadas. Es muy complicado que los receptores no sintonizados escuchar el trafico que se da en la Lan.

Complejas técnicas de encriptado hacen imposible para todos, incluso los más sofisticados, acceder de forma no autorizada al tráfico de la red. En general los nodos individuales deben tener habilitada la seguridad antes de poder participar en el tráfico de la red.

Costo

La instalación de una Lan inalámbrica incluye los costos de infraestructura para los puntos de acceso y los costes de usuario par los adaptadores de la red inalámbrica. Los costes de infraestructura dependen fundamentalmente del número de puntos de acceso desplegados. El valor de los puntos de acceso oscila entre 1000 y 2000 dólares. El número de puntos de acceso depende de la cobertura requerida y del número y tipo de usuarios.

El área de cobertura es proporcional al cuadrado del rango de productos adquirido. Los adaptadores son requeridos para las plataformas standard de ordenadores y su precio oscila entre 300 y 1000 dólares.

El coste de instalación y mantenimiento de una WLAN generalmente es más bajo que el costo de instalación y mantenimiento de una red cableada tradicional, por dos razones:

En primer lugar una red WLAN elimina directamente los costes de cableado y el trabajo asociado con la instalación y reparación.

En segundo lugar una red WLAN simplifica los cambios, desplazamientos y extensiones, por lo que se reducen los costes indirectos de los usuarios sin todo su equipo de trabajo y de administración.

Escalabilidad

Las redes WLAN pueden ser diseñadas para ser extremadamente simples o bastante complejas. WLAN's pueden soportar un amplio número de nodos y/o extensas áreas físicas añadiendo puntos de acceso para dar energía a la señal o para extender la cobertura.

Alimentación en las plataformas móviles

Los productos WLAN de los usuarios finales están diseñados para funcionar sin corriente alterna o batería de alimentación proveniente de sus portátiles, puesto que no tienen conexión propia cableada. Los fabricantes emplean técnicas especiales para maximizar el uso de la energía del computador y el tiempo de vida de su batería.

Seguridad laboral

La potencia de salida de los sistemas WLAN es muy baja, mucho menor que la de un teléfono móvil. Puesto que las señales de radio se atenuan rápidamente con la distancia, la exposición a la energía de radiofrecuencia en el área de la WLAN es muy pequeña. Las WLAN's deben cumplir las estrictas normas de seguridad dictadas por el gobierno y la industria. No se han atribuido nunca efectos secundarios en la salud a causa de una WLAN.

ADIÓS A LOS DICHOSOS CABLES

El sueño es eliminar los cables, y de momento despejar bastante la mesa ya es una realidad. Si contamos cables de datos en un ordenador doméstico (monitor, teclado, ratón, impresora, *joystick*, Internet, altavoces, etc) veremos que hay mucho que eliminar. En todas las distancias se han creado sistemas, basados en radio, para transmitir datos a través del aire.

Distancias cortas: Bluetooth

Tiene nombre de rey danés, es un estándar, ha tardado demasiado y está diseñado para despejar mesas. La idea de Bluetooth es ser barato, consumir poca batería y alcanzar un máximo de 10 metros, para sustituir los cables que conectan teléfonos móviles, PDAs u ordenadores entre sí o con todo tipo de periféricos.

También se usa en redes de área local (LANs), y en ´manos libres´ de coche. Bluetooth utiliza la banda 2.45 GHz del espectro radiofónico, que es abierta (no necesita licencia) y por tanto está muy saturada; para evitar interferencias usa técnicas especiales. Bluetooth también puede verificar la conexión entre dos aparatos mediante encriptación. La capacidad de la versión 2.0, que llegará este año al mercado, es de 2 Mb/sg. Se conocen fallos de seguridad que podrían servir para robar datos. También se conoce un virus que afecta a teléfonos con sistema operativo Symbian, aunque ambos problemas son en la práctica muy restringidos.

Distancias medias: WiFi

Diseñado para redes de área local, IEEE 802.11 es un protocolo abierto que nadie se tomaba en serio. Empresas pequeñas y ´hackers´ empezaron a usarlo, y pronto la versión ´b´, capaz de velocidades de 11 Mb/sg (mejor que ADSL o cable, peor que una LAN) se extendió mucho.

Su popularidad mejoró con la **versión ´g´**, capaz de 54 Mb/sg, y con el nuevo nombre de WiFi. Hoy es un sistema común en la empresa y se abre camino en el hogar.

WiFi ´b´ y ´g´ usan la banda de 2.45 GHz (la misma que Bluetooth, los microondas y muchos inalámbricos), y alcanza 40 metros en interiores y cerca de 100 en exteriores, aunque con antenas especiales se han conseguido enlaces punto a punto de más de 100 kilómetros.

Una instalación WiFi consta de un Punto de Acceso conectado al módem o ´router´ ADSL o de cable (a veces va incluido en el propio ´router´), y una tarjeta WiFi por ordenador. Estas tarjetas pueden ser internas, o de quita y pon como las PCMCIA de los portátiles. El punto de acceso emite y recibe de tal modo que varios ordenadores comparten la salida a Internet sin problemas (ni configuraciones).

Un ordenador con WiFi detecta automáticamente su presencia, y pregunta al usuario si se quiere conectar.

El principal inconveniente de WiFi es la seguridad; sus protocolos de control de acceso no son muy robustos. Lo cierto es que mucha gente deja sus redes abiertas, a propósito o por descuido, como forma de compartir su acceso a la Red. Así es muy normal encontrar redes WiFi abiertas. Las telefónicas no son felices.

Distancias amplia: WiMax

WiMax representa una evolución en lo referido a conexiones inalámbricas. El sistema más difundido hoy día para las conexiones inalámbricas de internet es el Wi-Fi.

El WiMax, cuyas siglas provienen de Worldwide Interoperability Microwave Access, o en español Interoperabilidad Mundial para el Acceso por Microondas, supone una evolución con respecto al Wi-Fi.

Ventajas de WiMax por sobre el Wi-Fi:
* Mayor alcance de cobertura
* Mayor velocidad de conexión

Mientras que la cobertura en un sistema tipo Wi-Fi va de los 50 a los 100 metros, con la tecnología WiMax se alcanza de 40 a 100 kilómetros. Esto permite extender el alcance de Internet inalámbrico a situaciones geográficas donde es complicado o imposible realizar un cableado convencional.

Con respecto a la velocidad de conexión, mientras que con Wi-Fi se tiene una velocidad teórica de 56 Mbps como velocidad máxima (con el estándar actual más difundido), la tecnología WiMax alcanza 128 Mbps de velocidad teórica.

Junto con estos 2 puntos se encuentra el mayor ancho de banda, lo que permite transmitir para varios equipos o estaciones conectadas y ejecutando más de un servicio en forma simultánea, como ser Telefonía IP, transmisión de video, imágenes, audio, etc.

Aunque este sistema de conexión todavía se encuentre en desarrollo (el principal escollo aparenta ser la estandarización y certificación de los equipos), seguramente será un gran salto con innumerables beneficios; quizás el más importante sería tener acceso en tiempo real a la información necesaria en situaciones límites donde se vea comprometida la vida, como ser rescates en zonas muy complicadas o también cubrir toda un área de una ciudad permitiendo tener conexión continua a Internet.

GLOSARIO DE TÉRMINOS
Punto de acceso: Dispositivo que transporta datos entre una red inalámbrica y una red cableada (infraestructura).
IEEE802.X: Conjunto de especificaciones de la redes LAN dictadas por el IEEE (the Institute of Electrical and Electronic Engineers). La mayor parte de las redes cableadas cumplen la norma 802.3, especificación para las redes ethernet basadas en CSMA/CD, o la norma 802.5, especificación para las redes Token Ring.
Existe un comité 802.11 trabajando en una normativa para redes inalámbricas de 1 y 2 Mbps. La norma tendrá una única capa MAC para las siguientes tecnologías: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) e infrarrojos. Se están desarrollando borradores de las normas.
Red independiente: Red que proporciona (normalmente temporalmente) conectividad de igual a igual sin depender de una infraestructura completa de red.
Infraestructura de red: Red inalámbrica centrada en un punto de acceso. En este entorno los puntos de acceso no solo proporcionan comunicación con la red cableada sino que también median el tráfico de red en la vecindad inmediata.
Microcélula: El espacio físico en el que un número de dispositivos de redes inalámbricas pueden comunicarse. Puesto que es posible tener células solapándose así como células aisladas los saltos entre células están establecidos por alguna regla.
Multipath: La variación de la señal causada cuando las señales de radio toman varios caminos desde el transmisor al receptor.

Términos de radio frecuencia: GHz, MHz, Hz.: La unidad internacional de medida de frcuencia es el Hertzio (Hz) el cual es equivalente a la unidad antigua de ciclos pos segundo. Un MHz es un millón de Hertzios y un GHz son mil MHz (mil millones de Hz). Como referencia: La frecuencia eléctrica utilizada en Europa son 50 Hz y en EEUU son 60 Hz. La banda de frecuencia de radiodifusión AM es 0.55 - 1.6 MHz. La banda de frecuencia de radiodifusión FM es 88 – 108 MHz. Los hornos microondas típicamente operan a 2.45 GHz.
Roaming: Movimiento de un nodo inalámbrico entre dos microcélulas. Roaming se da normalmente en infraestructuras de redes construidas con varios puntos de acceso.
Nodo inalámbrico: Ordenador de usuario con una tarjeta de red inalámbrica (adaptador).

Red privada virtual

Resumido de Wikipedia, la enciclopedia libre

Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red de área local (LAN) sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. **Todo ello utilizando la infraestructura de Internet.**

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar los aspectos fundamentales en cualquier comunicación:

1) Autentificación.
2) Integridad.
3) Confidencialidad.
4) No repudio.

1) Autenticación

Autenticación (*derivado del griego αυθεντικός = verdadero o genuino, de ' los authentes' = el autor*) o autentificación (*derivado del verbo autenticar*) es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, o sobre la cosa son verdadero. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad.

En términos de seguridad de redes de datos, a la **Autenticación** o **autentificación**, se la puede considerar como un proceso de tres pasos fundamentales que se resumen en lo siguiente:

a) La **Autenticación** es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa una PC, una PC por sí mismo o un programa de PC. En una web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.
b) A la autenticación le sigue la **Autorización** que la definimos como el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
c) Finalmente mediante la **Auditoría** la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autenticado, autorizados o no.

2) Integridad

La Integridad hace referencia a que los datos transmitidos no han sido alterados. Para ello normalmente se utiliza funciones de Hash. Una función de Hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. Una propiedad fundamental de la función de hash es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son. Es posible que existan claves resultantes iguales para objetos diferentes, ya que el rango de posibles claves es mucho menor que el de posibles objetos a resumir.

3) Confidencialidad

Dado que los datos viajan a través de un medio tan inseguro como Internet, dichos datos son susceptibles de intercepción, por lo que resulta fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Para ello se hace uso de algoritmos de cifrado.

4) No repudio

El no repudio de una comunicación hace referencia a que no puede negar que el mensaje lo envió el emisor.

Requerimientos básicos de una Red Privada Virtual (VPN)

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Codificación de datos: los datos que se van a transmitir a través de la red pública (Internet), deben ser cifrados, para que así no puedan ser leídos por terceros que puedan ver el tráfico de los datos. Esta tarea se realiza con algoritmos de cifrado que son estudiados por la criptografía.
- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

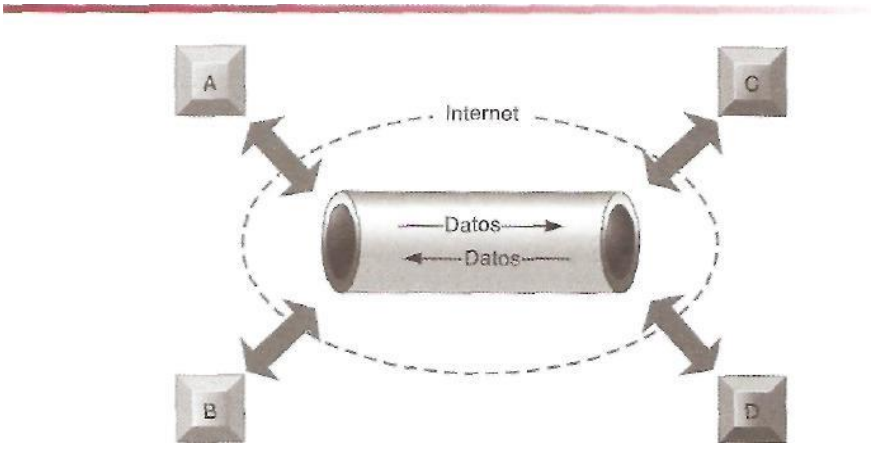
Tipos de Redes Privadas Virtuales

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto: Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etc.) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos tradicionales punto a punto, sobre todo en las comunicaciones internacionales. La más común es la tecnología de túnel o “tunneling” que utiliza el protocolo PPTP (Protocolo de Túnel de Punto a Punto). Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos. Los paquetes de datos se encriptan y encapsulan dentro de los paquetes IP de la Internet.

RED PRIVADA VIRTUAL QUE UTILIZA INTERNET



Esta VPN es una red privada de computadoras enlazadas utilizando una conexión segura de "túnel" a través de Internet. La red protege los datos transmitidos sobre la Internet pública codificándolos y "encapsulándolos" dentro del Protocolo Internet (IP). Al agregar una cápsula alrededor de un mensaje de red para ocultar su contenido, las organizaciones pueden crear una conexión privada que viaje a través de la Internet pública.

VPN interna, VLAN: Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio

de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi). Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Ventajas

Podemos destacar tres ventajas:

1) Integridad, confidencialidad y seguridad de datos.
2) Las VPN reducen los costos y son sencillas de usar.
3) Facilita la comunicación entre los usuarios en lugares distantes a muy bajo costo.

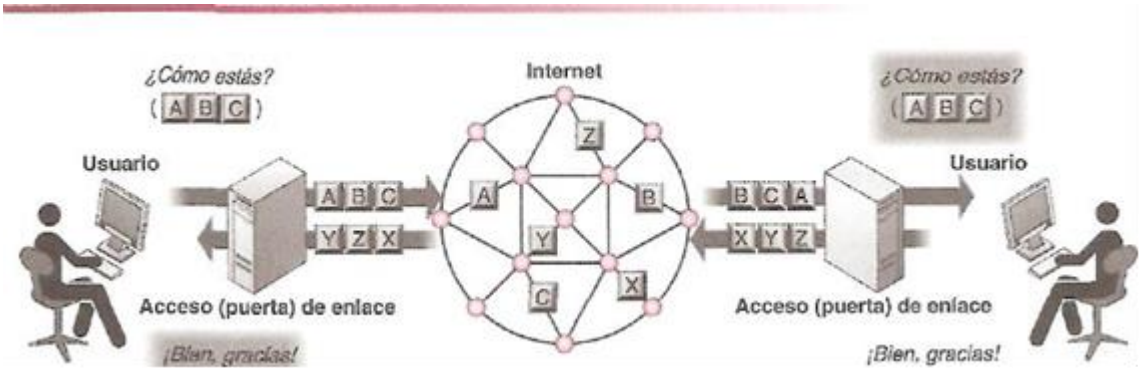
Telefonía por Internet (VoIP)

Sistemas de Información Gerencial (Laudon y Laudon – Edición X)

La telefonía por Internet permite a las empresas utilizar tecnología de Internet para la transmisión telefónica de voz por Internet o redes privadas. (Los productos de telefonía por Internet a veces se denominan productos de telefonía IP). La tecnología voz sobre IP (VoIP) utiliza el Protocolo Internet (IP) para transmitir información de voz en forma digital utilizando conmutación de paquetes, y evitando de esta manera las tarifas que cobran las redes telefónicas locales y de larga distancia. Las llamadas que comúnmente serían transmitidas por las redes telefónicas públicas podrían viajar a través de la red corporativa basada en el Protocolo Internet o la Internet pública. Las llamadas de telefonía IP se pueden realizar y recibir con una computadora de escritorio equipada con un micrófono y bocinas o con un teléfono habilitado para VoIP.
VoIP es el tipo de servicio telefónico de más rápido crecimiento en Estados Unidos. El número de líneas casi se está duplicando cada año y se espera que para el año 2008 llegue a 30 millones (eMarketer, 2005c). Vonage, el primer impulsor de VoIP, compite con las empresas telefónicas regionales (como Verizon) y las empresas de cable (como Timer Warner y Cablevision). Skype, que ofrece VoIP gratuita en todo el mundo a través de una red de igual a igual, fue adquirida por eBay y Google cuenta con su propio servicio VoIP gratuito.

A pesar de que se requieren inversiones por adelantado para un sistema telefónico IP, VoIP puede reducir de 20 a 30 por ciento los costos de las comunicaciones y de administración de la red. Por ejemplo, VoIP ahorra al Virgin Entertainment Group 700,000 dólares anuales en cargos de larga distancia (Hoover, 2006). Además de reducir los costos de larga distancia y eliminar tarifas mensuales por líneas privadas, una red IP proporciona una sola infraestructura de voz y datos para los servicios de telecomunicaciones y computación. Las empresas ya no tienen que mantener redes separadas o proporcionar servicios de soporte técnico y personal para cada tipo distinto de red.

Otra ventaja de VoIP es su flexibilidad. A diferencia de la red telefónica tradicional, los teléfonos se pueden agregar o cambiar de oficinas sin necesidad de volver a tender cableado o reconfigurar la red. Con VoIP, una llamada de conferencia se puede realizar con una simple operación de hacer clic y arrastrar en la pantalla de la computadora para seleccionar los nombres de los participantes. El correo de voz y el correo electrónico se pueden combinar en un solo directorio.



Una llamada telefónica IP digitaliza y divide un mensaje de voz en paquetes de datos que podrían viajar a través de diferentes rutas antes de re-ensamblarse en su destino final. Un procesador cercano al destino de la llamada, denominado acceso (o puerta) de enlace, ordena los paquetes en el orden correcto y los redirige al número telefónico del receptor o a la dirección IP de la computadora receptora.

LA REVOLUCIÓN INALÁMBRICA

Sistemas de Información Gerencial (Laudon y Laudon – Edición X)

Si usted cuenta con un teléfono celular, ¿lo emplea para tomar y enviar fotografías, enviar mensajes de texto o descargar videos clips de música? ¿Lleva su computadora portátil a la escuela o a la biblioteca para enlazarse a Internet? Si lo hace, ¡usted es parte de la revolución inalámbrica! Los teléfonos celulares, las computadoras portátiles y los pequeños dispositivos de mano se han tornado en plataformas de cómputo portátiles que le permiten realizar algunas de las tareas de cómputo que usted acostumbraba realizar en su escritorio.

La comunicación inalámbrica ayuda a las empresas a mantenerse en contacto más fácilmente con clientes, proveedores y empleados y ofrece formas más flexibles para organizar el trabajo. La tecnología inalámbrica también ha creado nuevos productos, servicios y canales de ventas.

DISPOSITIVOS INALÁMBRICOS

Si usted requiere comunicación móvil y potencia de cómputo o acceso remoto a sistemas corporativos, puede trabajar con una variedad de dispositivos inalámbricos: PCs, teléfonos celulares, asistentes digitales personales (PDAs), dispositivos de correo electrónico y teléfonos inteligentes. Los asistentes digitales personales (PDAs) son pequeñas computadoras de mano que ofrecen aplicaciones como agendas electrónicas, libretas de direcciones, bloc de notas y controlador de gastos. Muchos modelos presentan mensajería por correo electrónico, acceso inalámbrico a Internet, comunicación de voz y cámaras digitales. Los dispositivos de correo electrónico portátil, como el BlackBerry Handheld, están optimizados para la mensajería de texto inalámbrica. Los dispositivos híbridos que combinan la funcionalidad de un PDA con la de un teléfono celular digital se conocen como teléfonos inteligentes (smartphones).

SISTEMAS CELULARES

Los teléfonos celulares no sólo son para comunicación de voz: se han convertido en plataformas móviles para la entrega de datos digitales. Los teléfonos móviles permiten que muchos millones de personas se comuniquen y accedan a Internet en África y otros países donde el teléfono convencional o el servicio de Internet es costoso o no está disponible.

Estándares y generaciones de redes celulares

El servicio celular digital utiliza varios estándares contrapuestos que son incompatibles. Esto significa que los equipos celulares digitales no funcionan en redes que utilizan otro estándar inalámbrico.

En Europa y en gran parte del resto del mundo, excepto Estados Unidos, el estándar es el Sistema Global para la Comunicación Móvil (GSM). La fortaleza de GSM es su capacidad de roaming internacional. Los usuarios tienen roaming sin problemas con el mismo número en más de 170 países. La mayoría de los sistemas GSM fuera de Estados Unidos operan en las bandas de frecuencia de 900 MHz y 1.8 gigahertz (GHz). (En Estados Unidos operan en la banda de 1.9 GHz).

Existen sistemas telefónicos celulares GSM en Estados Unidos, como T-Mobile y Cingular; sin embargo, el estándar más utilizado en ese país es el Acceso Múltiple por División de Código (CDMA), que es el sistema utilizado por Verizon y Sprint. CDMA fue desarrollado por las fuerzas armadas durante la Segunda Guerra Mundial. Transmite sobre diversas frecuencias, ocupa todo el espectro y con el tiempo asigna usuarios al azar a un rango de frecuencias. En general, la implementación de CDMA es menos costosa, su uso del espectro es más eficiente y proporciona una mayor calidad de voz y datos que GSM.

GENERACIONES DE CELULARES

La mayoría de los sistemas celulares digitales actuales se utilizan principalmente para voz, pero tienen la capacidad para transmitir datos a velocidades que van de 9.6 a 2 Mbps. La mayoría de los usuarios de celulares de Estados Unidos con servicio Web adquieren planes que ofrecen 384 Kbps, que es una velocidad aceptable para correo electrónico pero no para descargar archivos grandes o páginas Web completas. El uso más económico de la tecnología de celulares para transmisión de datos es la mensajería SMS. El servicio de mensajes breves (SMS) es un servicio de mensajes de texto utilizado por numerosos

sistemas de teléfonos celulares digitales para enviar y recibir mensajes alfanuméricos breves menores a 160 caracteres de longitud. Al igual que el correo electrónico, los mensajes SMS se pueden reenviar y almacenar para recuperarlos posteriormente.

Las redes celulares más potentes llamadas redes de tercera generación (3G) tienen velocidades de transmisión que varían de 384 Kbps para usuarios móviles en, digamos, un automóvil, a más de 2 Mbps para usuarios fijos. Esta capacidad de transmisión es suficiente para video, gráficos y otros medios enriquecidos, además de voz, lo cual hace a las redes 3G adecuadas para el acceso inalámbrico y de banda ancha a Internet y para la transmisión constante de datos.

Las empresas de servicios inalámbricos están empezando a introducir servicios 3G. Mientras tanto, a quienes les interesa el acceso a Internet y la transmisión de datos de alta velocidad donde no se dispone de 3G, están recurriendo a una solución intermedia denominada redes 2.5G. Estas redes utilizan actualizaciones a la infraestructura celular existente y presentan velocidades de transmisión de datos que varían de 30 a 144 Kbps.

Estándares inalámbricos móviles para el acceso a la Web
También hay múltiples estándares y tecnologías que rigen la manera en que los teléfonos celulares acceden a Internet y la World Wide Web. El Protocolo de Aplicaciones Inalámbricas (WAP) es un sistema de protocolos y tecnologías que permite a los teléfonos celulares y otros dispositivos inalámbricos con diminutas pantallas, conexiones de bajo ancho de banda y memoria mínima, acceder a información y servicios basados en la Web. WAP utiliza el Lenguaje de Marcación Inalámbrico (WML), que se basa en XML y está optimizado para pantallas diminutas.

Una persona con un teléfono que se apega a WAP utiliza el micronavegador integrado para realizar una solicitud en WML. Un micronavegador es un navegador de Internet con un tamaño de archivo pequeño que se adapta a las restricciones de escasa memoria de los dispositivos inalámbricos portátiles y al poco ancho de banda de las redes inalámbricas. La solicitud se pasa a un acceso de enlace WAP, la cual recupera la información de un servidor de Internet en formato HTML estándar o en WML. El acceso de enlace traduce el contenido HTML a WML para que lo reciba el cliente WAP. Este protocolo soporta la mayoría de los estándares para redes inalámbricas y los sistemas operativos para dispositivos de cómputo portátiles.
I-mode es un servicio inalámbrico ofrecido por la red telefónica móvil NTT Do-CoMo de Japón, que utiliza un conjunto diferente de estándares. En lugar de utilizar WAP, i-mode emplea HTML compacto para entregar contenido, lo cual facilita a las empresas convertir sus sitios Web HTML a servicio móvil. I-mode permite a los usuarios permanecer conectados constantemente a la red y a los proveedores de contenido difundir información relevante a los usuarios. (Los usuarios de WAP tienen que marcar para revisar si un sitio ha cambiado).

REDES DE COMPUTADORAS INALÁMBRICAS Y ACCESO A INTERNET

Si usted tiene una computadora portátil, podría utilizarla para acceder a Internet a medida que se desplaza de una habitación a otra de su dormitorio, o de una mesa a otra en la biblioteca de su universidad. Un conjunto de tecnologías proporcionan acceso inalámbrico de alta velocidad a Internet para PCs y otros dispositivos inalámbricos portátiles, al igual que para teléfonos celulares. Estos nuevos servicios de alta velocidad han extendido el acceso a Internet a numerosos lugares que no podrían ser abarcados por los tradicionales servicios de Internet alámbricos.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha establecido una jerarquía de estándares complementarios para redes de computadoras inalámbricas. Estos estándares incluyen el IEEE 802.15 para la red de área personal (Bluetooth), el IEEE 802.11 para la red de área local (LAN; WiFi) y el 802.16 para la red de área metropolitana (MAN; WiMax).

Bluetooth
Bluetooth es el nombre popular para el estándar de conectividad de redes inalámbrica 802.15, útil para crear pequeñas redes de área personal (PANs). Este estándar enlaza hasta ocho dispositivos dentro de un área de 10 metros utilizando comunicaciones basadas en radio de baja potencia y puede transmitir hasta 722 Kbps en la banda de 2.4 GHz.

Los teléfonos, localizadores, computadoras, impresoras y dispositivos de cómputo inalámbricos que utilizan Bluetooth se comunican entre sí e incluso operan entre sí sin intervención directa del usuario (vea la figura 7-16). Por ejemplo, una persona podría emplear una computadora portátil para enviar de manera inalámbrica un archivo de documento a una impresora. Bluetooth conecta teclados y ratones inalámbricos a

PCs o teléfonos celulares a audífonos sin alambres. Bluetooth tiene bajos requerimientos de potencia, lo cual lo hace apropiado para computadoras portátiles, teléfonos celulares y PDAs que utilizan baterías.
Aunque Bluetooth es propicio para la conectividad de redes personal, tiene usos en grandes corporaciones. Por ejemplo, los conductores de Federal Express utilizan Bluetooth para transmitir los datos de entrega capturados por sus computadoras portátiles PowerPad a transmisores celulares, los cuales reenvían los datos a las computadoras corporativas. Los conductores ya no requieren invertir tiempo para acoplar físicamente sus unidades portátiles en los transmisores, y Bluetooth ha ahorrado a FedEx 20 millones de dólares anuales.

Wi-Fi

El conjunto de estándares IEEE para LANs inalámbricas es la familia 802.11, también conocida como Wi-Fi (fidelidad inalámbrica). Existen tres estándares en esta familia: 802.11a, 802.11b y 802.11g. El 802.11n es un estándar emergente para incrementar la velocidad y capacidad de la conectividad de redes inalámbrica.
El estándar 802.11a puede transmitir hasta 54 Mbps en el rango de frecuencia de 5 GHz no autorizado y tiene una distancia efectiva de 10 a 30 metros. El estándar 802.11b puede transmitir hasta 11 Mbps en la banda de 2.4 GHz no autorizada y tiene una distancia efectiva de 30 a 50 metros, aunque este alcance se puede extender al exterior por medio de antenas montadas en torres. El estándar 802.11g puede transmitir hasta 54 Mbps en el rango de 2.4 GHz. El 802.11n transmitirá a más de 200 Mbps.

Debido a que 802.11b y 802.11g operan en la frecuencia de 2.4 GHz, los productos construidos para cualquiera de estos dos estándares son compatibles. Los productos diseñados para la especificación 802.11a no funcionarán con el 802.11b ni con el 802.11g, a consecuencia de que el 802.11a utiliza una banda de frecuencia diferente.

El 802.11b fue el primer estándar inalámbrico ampliamente adoptado para LANs inalámbricas y acceso inalámbrico a Internet. El 802.11g se utiliza cada vez más con este propósito, y ya existen sistemas de banda dual capaces de manejar el 802.11b y el 802.11g.

Un sistema Wi-Fi puede operar en dos modos diferentes. En modo de infraestructura, los dispositivos inalámbricos se comunican con una LAN alámbrica a través de puntos de acceso. Un punto de acceso es una caja que consta de un radio receptor/transmisor y antenas que enlazan con una red alámbrica, un ruteador o un concentrador.

En modo con fines específicos, también denominado modo de punto a punto, los dispositivos inalámbricos se comunican entre sí directamente y no requieren un punto de acceso. La mayoría de las comunicaciones Wi-Fi utilizan el modo de infraestructura. (El modo con fines específicos se utiliza para LANs muy pequeñas en el hogar o en oficinas de pequeñas empresas).

La mayoría de los dispositivos inalámbricos son computadoras cliente. Los servidores que las estaciones cliente móviles requieren utilizar están en la LAN alámbrica. El punto de acceso controla las estaciones inalámbricas y sirve como puente entre la LAN alámbrica principal y la LAN inalámbrica. (Un puente conecta dos LANs basadas en diferentes tecnologías). El punto de acceso también controla las estaciones inalámbricas.

Las estaciones inalámbricas móviles con frecuencia necesitan una tarjeta complementaria denominada tarjeta de interfaz de red inalámbrica (NIC) que tiene un radio y una antena integrados. Las NICs inalámbricas pueden ser del tamaño de una tarjeta de crédito que se encajan en la ranura PCMCIA (Asociación Internacional de Tarjetas de Memoria para Computadora Personal, que también se conoce como ranura para tarjeta de PC) de una PC o en adaptadores externos que se conectan en el puerto USB (bus serial universal) de la PC. Las PCs portátiles más recientes traen chips integrados que pueden recibir señales Wi-Fi.

Wi-Fi y acceso inalámbrico a Internet

El estándar 802.11 también proporciona acceso inalámbrico a Internet por medio de una conexión de banda ancha. En este caso, un punto de acceso se conecta en una conexión a Internet, que puede provenir de una línea de televisión por cable o el servicio telefónico DSL. Las computadoras que se encuentren dentro del alcance del punto de acceso lo utilizan para enlazarse de manera inalámbrica a Internet.

Las grandes corporaciones y las pequeñas empresas utilizan redes Wi-Fi para proporcionar LANs inalámbricas y acceso a Internet de bajo costo. Los puntos activos Wi-Fi están proliferando en hoteles, salas

de espera de aeropuertos, bibliotecas, cafés y campus universitarios para proporcionar acceso móvil a Internet.

Los puntos activos consisten comúnmente en uno o más puntos de acceso ubicados en un techo, una pared o en otro punto estratégico de un lugar público para proporcionar la máxima cobertura inalámbrica a un área específica. Los usuarios dentro del alcance de un punto activo pueden acceder a Internet desde sus computadoras portátiles. Algunos puntos activos son gratuitos o no requieren software adicional; otros podrían requerir activación y el establecimiento de una cuenta de usuario proporcionando un número de tarjeta de crédito en la Web.

No obstante, la tecnología Wi-Fi plantea varios retos. En la actualidad, los usuarios no pueden pasar libremente de un punto activo a otro si estos puntos activos utilizan servicios de red Wi-Fi distintos. A menos que el servicio sea gratuito, los usuarios tendrían que registrarse en cuentas separadas para cada servicio, cada uno con sus propias tarifas.

Una desventaja importante de Wi-Fi son sus débiles características de seguridad, que hacen a estas redes inalámbricas vulnerables a los intrusos.

Otra desventaja de las redes Wi-Fi es la susceptibilidad a interferencia por parte de sistemas cercanos que operen en el mismo espectro, como teléfonos inalámbricos, hornos de microondas u otras LANs inalámbricas. Las redes inalámbricas basadas en la especificación 802.11n solucionarán este problema utilizando múltiples antenas inalámbricas a la vez para transmitir y recibir datos, y una tecnología llamada MIMO (múltiple entrada múltiple salida) para coordinar múltiples señales de radio simultáneas.

WiMax

Una cantidad sorprendentemente grande de áreas geográficas de Estados Unidos y de todo el mundo no tienen acceso a conectividad Wi-Fi o de banda ancha fija. El alcance de los sistemas Wi-Fi no es mayor de 91 metros desde la estación base, lo cual dificulta que los grupos rurales que no cuentan con servicio de cable o DSL tengan acceso inalámbrico a Internet.

El IEEE desarrolló una nueva familia de estándares conocida como WiMax para enfrentar estos problemas. Wi-Max, que significa Interoperabilidad Mundial para el Acceso por Microondas, es el término popular para el estándar 802.16 del IEEE, conocido como "Interfaz Aérea para Sistemas Fijos de Acceso Inalámbrico de Banda Ancha". Wi-Max tiene un alcance de acceso inalámbrico de hasta 50 kilómetros, comparado con los 91 metros de Wi-Fi y los 10 metros de Bluetooth, y una tasa de transferencia de datos de hasta 75 Mbps. La especificación 802.16 tiene una seguridad robusta y características de calidad de servicio para soportar voz y video.

Las antenas WiMax son suficientemente potentes para transmitir conexiones a Internet de alta velocidad a antenas colocadas en los techos de casas y empresas que se encuentren a varios kilómetros de distancia. Spring Nextel está construyendo una red WiMax nacional para soportar video, llamadas de video y otros servicios inalámbricos de uso intensivo de datos, e Intel tiene unos chips especiales que facilitan el acceso WiMax desde computadoras móviles.

Servicios inalámbricos de banda ancha celular y servicios inalámbricos emergentes

Suponga que su fuerza de ventas necesita acceder a la Web o utilizar correo electrónico pero no siempre encuentra un punto activo Wi-Fi conveniente. Ahora puede conectar una pequeña tarjeta en su computadora portátil y utilizar su PC en una red celular. Las principales empresas telefónicas celulares han configurado sus redes 3G para proporcionar acceso de banda ancha en cualquier momento y cualquier lugar a PCs y otros dispositivos portátiles. Cingular ofrece un servicio llamado EDGE. El servicio de Verizon se llama BroadBand Access y se basa en una tecnología llamada **EV-DO**, que significa Evolución de optimización de datos. EV-DO proporciona acceso inalámbrico a Internet sobre una red celular a una velocidad promedio de 300 a 500 Kbps. Sprint ofrece un servicio inalámbrico similar a EV-DO.

Los teléfonos celulares, los PDAs inalámbricos y las computadoras portátiles ofrecen cada vez más la capacidad de cambiar de un tipo de red a otro. Por ejemplo, la mayoría de los nuevos teléfonos celulares actuales tienen capacidades de Blue¬tooth o la capacidad para soportar llamadas inalámbricas por Internet.

RFID Y REDES DE SENSORES INALÁMBRICOS

Las tecnologías móviles están creando nuevas eficiencias y formas de trabajar en toda la empresa. Además de los sistemas inalámbricos que acabamos de describir, los sistemas de identificación por radiofrecuencia (RFID) y las redes de sensores inalámbricos están teniendo un mayor impacto.

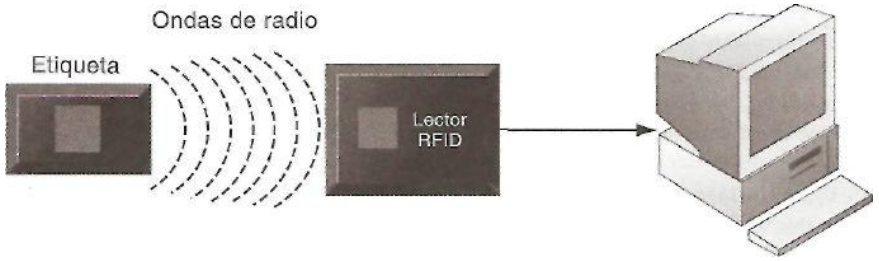
Identificación por radiofrecuencia (RFID)

Los sistemas de identificación por radiofrecuencia (RFID) proporcionan una tecnología poderosa para rastrear el desplazamiento de bienes por toda la cadena de suministro. Los sistemas RFID utilizan diminutas etiquetas con microchips incrustados que contienen datos acerca de un artículo y su localización para transmitir señales de radio a través de una distancia corta a lectores RFID especiales. Estos lectores pasan los datos sobre una red a una computadora para su procesamiento. A diferencia de los códigos de barras, las etiquetas RFID no requieren ser vistas directamente para poder leerlas.

La etiqueta RFID, se programa electrónicamente con información que identifica de manera única a un artículo, más información adicional como su ubicación, dónde y cuándo se fabricó o su estado durante la producción. En la etiqueta se encuentra un microchip incrustado para almacenar los datos. El resto de la etiqueta es una antena que transmite datos al lector.

La unidad lectora consta de una antena y un transmisor de radio con una función para decodificar adjunta a un dispositivo fijo o portátil. El lector emite ondas de radio con un alcance desde 2.5 centímetros hasta 30 metros, dependiendo de su potencia de salida, la radiofrecuencia empleada y las condiciones ambientales. Cuando una etiqueta RFID está dentro del alcance de un lector, se activa y comienza a enviar datos. El lector capta estos datos, los decodifica y los envía a una computadora host a través de una red alámbrica o inalámbrica para su procesamiento (vea la figura 7-18). Tanto las etiquetas como las antenas RFID se fabrican en varias formas y tamaños.

Los sistemas RFID operan en diversas bandas de frecuencia no autorizadas en todo el mundo. Los sistemas de baja frecuencia (de 30 a 500 kilohertz) tienen alcances de lectura cortos (de centímetros a unos cuantos metros); costos bajos del sistema, y con frecuencia se utilizan en aplicaciones de seguridad, seguimiento de activos o identificación de animales. Los sistemas RFID de alta frecuencia (de 850 a 950 MHz y 2.4 a 2.5 GHz) ofrecen alcances de lectura que se pueden extender más allá de 27 metros y son útiles para aplicaciones como seguimiento de vagones de ferrocarril o cobro automatizado de peaje en autopistas o puentes.



RFID utiliza transmisores de radio de baja potencia para leer los datos almacenados en una etiqueta a distancias que van de 2.5 centímetros a 30 metros. El lector captura los datos de la etiqueta y los envía a través de una red a una computadora host para su procesamiento.

En control de inventarios y administración de la cadena de suministro, los sistemas RFID captan y manipulan la información más detallada acerca de artículos que se encuentran en almacenes o en producción que los sistemas de códigos de barras. Si se embarca una gran cantidad de artículos, los sistemas RFID rastrean cada tarima, lote o incluso cada artículo unitario del embarque. Los fabricantes que utilizan RFID podrán rastrear el historial de producción de cada producto para una mejor comprensión de los defectos y éxito de los productos.

RFID ha estado disponible durante décadas, pero su uso generalizado se retrasó por lo costoso de las etiquetas, que van desde menos de 1 dólar a 20 dólares cada una. En la actualidad el costo de una etiqueta ha caído a cerca de 19 centavos de dólar y dentro de pocos años descenderá a 5 centavos de dólar. A estos precios por etiqueta, RFID se vuelve rentable para muchas empresas.

Además de instalar lectores RFID y sistemas de etiquetado, las empresas tendrían que actualizar su hardware y software para procesar las grandes cantidades de datos que producen los sistemas RFID — transacciones que podrían llegar a decenas o cientos de terabytes.

Se requiere middleware especial para filtrar, agregar e impedir que los datos de RFID sobrecarguen las redes empresariales y las aplicaciones de sistemas. Las aplicaciones necesitan rediseñarse para aceptar con frecuencia enormes volúmenes de datos generados por RFID y para compartirlos con otras aplicaciones. Los principales desarrolladores de software empresarial, como SAP y Oracle-PeopleSoft, actualmente ofrecen versiones habilitadas para RFID de sus aplicaciones de administración de la cadena de suministro.

La Sesión Interactiva sobre Organizaciones trata estos temas. Wal-Mart ha requerido a sus principales proveedores que utilicen etiquetas RFID pasivas en las cajas y tarimas embarcadas a sus almacenes para ayudar a rastrear y registrar el flujo de inventario. Los proveedores han procedido con lentitud por las dificultades en la implementación de RFID.

Redes de sensores inalámbricos

Si su empresa quisiera tecnología de punta para supervisar la seguridad del edificio o detectar sustancias peligrosas en el aire, podría implementar una red de sensores inalámbricos. Las redes de sensores inalámbricos (WSNs) son redes de dispositivos inalámbricos interconectados que se distribuyen en el entorno físico para proporcionar mediciones de una gran variedad a través de grandes espacios. Estos dispositivos tienen integrados sensores y antenas de procesamiento, almacenamiento y radiofrecuencia. Todos están enlazados en una red interconectada que envía los datos que detectan a una computadora para su análisis.

Estas redes varían de cientos a miles de nodos. Debido a que los dispositivos sensores inalámbricos se colocan en el campo una sola vez para que duren años sin ningún tipo de mantenimiento ni intervención humana, deben tener bajos requerimientos de energía y baterías capaces de durar varios años.

Por lo general, las redes de sensores tienen una arquitectura en capas, como la que emplea el sistema de seguridad inalámbrico ilustrado en la figura 7-19. Esta red de sensores inalámbricos en particular empieza con sensores de bajo nivel y progresa hacia nodos para agregación, análisis y almacenamiento de datos de alto nivel. Tanto los datos simples como los complejos se envían a través de la red a una instalación automatizada que proporciona vigilancia y control continuos del edificio.

Las redes de sensores inalámbricos son valiosas en áreas como la vigilancia de cambios ambientales; la vigilancia del tráfico o de la actividad militar; la protección de la propiedad; la operación y manejo eficiente de maquinaria y vehículos; el establecimiento de perímetros de seguridad; la vigilancia de la administración de la cadena de suministro; o la detección de material químico, biológico o radiológico.

Tipos de servidores

En las siguientes listas hay algunos tipos comunes de servidores y sus propósitos.

- **Servidor de archivos**: almacena varios tipos de archivo y los distribuye a otros clientes en la red.
- **Servidor de impresiones**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.
- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con *e-mail* para los clientes de la red.
- **Servidor de fax**: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
- **Servidor de la telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz,

almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o Internet; p. ej., la entrada excesiva del IP de la voz (VoIP), etc.

- **Servidor proxy**: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (por ejemplo., *prefetching* y depositar documentos u otros datos que se soliciten muy frecuentemente). También *sirve* seguridad; esto es, tiene un Firewall (cortafuegos). Permite administrar el acceso a Internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web.

- **Servidor del acceso remoto (RAS)**: controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos normalmente como contenido), y distribuye este contenido a clientes que la piden en la red.

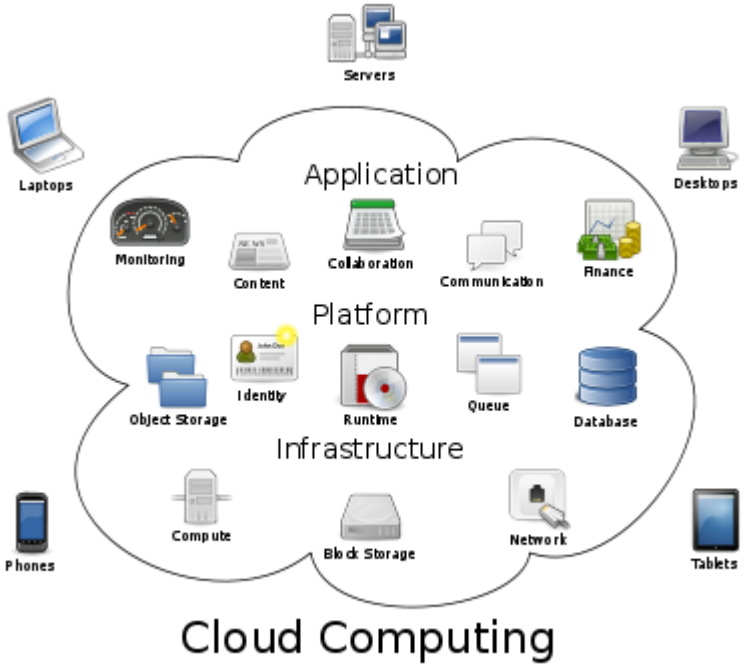
- **Servidor de reserva**: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada *clustering*.

- **Impresoras**: muchas impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un ***"print server"***, actuando como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión de ser terminado

- **Servidor de Autenticación**: Es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basándose en el estándar 802.1x y puede ser un servidor de tipo *RADIUS*.

- **Servidor DNS**: Este tipo de servidores resuelven nombres de dominio sin necesidad de conocer su dirección IP.

Computación en la nube (de Wikipedia, la enciclopedia libre)



La **computación en la nube** concepto conocido también bajo los términos **servicios en la nube**, **informática en la nube**, **nube de cómputo** o **nube de conceptos**, del inglés *Cloud computing*, es un paradigma que permite ofrecer servicios de computación a través de Internet.

Introducción

En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio,de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan. Según el IEEE Computer Society, es un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc.

"Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.

El cambio paradigmático que ofrece computación en nube es que permite aumentar el número de servicios basados en la red. Esto genera beneficios tanto para los proveedores, que pueden ofrecer, de forma más rápida y eficiente, un mayor número de servicios, como para los usuarios que tienen la posibilidad de acceder a ellos, disfrutando de la 'transparencia' e inmediatez del sistema y de un modelo de pago por consumo.

Computación en nube consigue aportar estas ventajas, apoyándose sobre una infraestructura tecnológica dinámica que se caracteriza, entre otros factores, por un alto grado de automatización, una rápida movilización de los recursos, una elevada capacidad de adaptación para atender a una demanda variable, así como virtualización avanzada y un precio flexible en función del consumo realizado evitando además el uso fraudulento del software y la piratería.

La computación en nube es un concepto que incorpora el software como servicio, como en la Web 2.0 y otros conceptos recientes, también conocidos como tendencias tecnológicas, que tienen en común el que confían en Internet para satisfacer las necesidades de cómputo de los usuarios.

Comienzos

El concepto de la computación en la nube empezó en proveedores de servicio de Internet a gran escala, como Google, Amazon AWS, Microsoft y otros que construyeron su propia infraestructura. De entre todos ellos emergió una arquitectura: un sistema de recursos distribuidos horizontalmente, introducidos como servicios virtuales de TI escalados masivamente y manejados como recursos configurados y mancomunados de manera continua. Este modelo de arquitectura fue inmortalizado por George Gilder en su artículo de octubre 2006 en la revista Wired titulado *Las fábricas de información*. Las granjas de servidores, sobre las que escribió Gilder, eran similares en su arquitectura al procesamiento "grid" (red, parrilla), pero mientras que las redes se utilizan para aplicaciones de procesamiento técnico débilmente acoplados (*loosely coupled*), un sistema compuesto de subsistemas con cierta autonomía de acción, que mantienen una interrelación continua entre ellos, este nuevo modelo de nube se estaba aplicando a los servicios de Internet.

Beneficios

- Integración probada de servicios Red. Por su naturaleza, la tecnología de "Cloud Computing" se puede integrar con mucha mayor facilidad y rapidez con el resto de sus aplicaciones empresariales (tanto software tradicional como Cloud Computing basado en infraestructuras), ya sean desarrolladas de manera interna o externa.[3]

- Prestación de servicios a nivel mundial. Las infraestructuras de "Cloud Computing" proporcionan mayor capacidad de adaptación, recuperación de desastres completa y reducción al mínimo de los tiempos de inactividad.

- Una infraestructura 100% de "Cloud Computing" permite al proveedor de contenidos o servicios en la nube prescindir de instalar cualquier tipo de hardware, ya que éste es provisto por el proveedor de la infraestructura o la plataforma en la nube. La belleza de la tecnología de "Cloud Computing" es su simplicidad… y el hecho de que requiera mucha menor inversión para empezar a trabajar.

- Implementación más rápida y con menos riesgos. Podrá empezar a trabajar muy rápidamente gracias a una infraestructura de "Cloud Computing". No tendrá que volver a esperar meses o años e invertir grandes cantidades de dinero antes de que un usuario inicie sesión en su nueva solución. Sus aplicaciones en tecnología de "Cloud Computing" estarán disponibles en cuestión de días o horas en lugar de semanas o meses, incluso con un nivel considerable de personalización o integración.

- Actualizaciones automáticas que no afectan negativamente a los recursos de TI. Si actualizamos a la última versión de la aplicación, nos veremos obligados a dedicar tiempo y recursos (que no tenemos) a volver a crear nuestras personalizaciones e integraciones. La tecnología de "Cloud Computing" no le obliga a decidir entre actualizar y conservar su trabajo, porque esas personalizaciones e integraciones se conservan automáticamente durante la actualización.

- Contribuye al uso eficiente de la energía. En este caso, a la energía requerida para el funcionamiento de la infraestructura. En los datacenters tradicionales, los servidores consumen mucha más energía de la requerida realmente. En cambio, en las nubes, la energía consumida es sólo la necesaria, reduciendo notablemente el desperdicio.

Desventajas

- La centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios.

- La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.

- Los datos "sensibles" del negocio no residen en las instalaciones de las empresas, lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.

- La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los proveedores de servicios en nube. Empresas emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.[4]

- La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.

- La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.

- Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que estos requieren.

- Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o jitter altos.

Capas

Software como servicio

El software como servicio (en inglés *software as a service*, SaaS) se encuentra en la capa más alta y caracteriza una aplicación completa ofrecida como un servicio, en-demanda, vía multitenencia —que significa una sola instancia del software que corre en la infraestructura del proveedor y sirve a múltiples organizaciones de clientes. El ejemplo de SaaS conocido más ampliamente es Salesforce.com, pero ahora ya hay muchos más, incluyendo las Google Apps que ofrecen servicios básicos de negocio como el e-mail. Por supuesto, la aplicación multitenencia de Salesforce.com ha constituido el mejor ejemplo de cómputo en nube durante unos cuantos años. Por otro lado, como muchos otros jugadores en el negocio del cómputo en nube, Salesforce.com ahora opera en más de una capa de la nube con su Force.com, que ya está en servicio, y que consiste en un ambiente de desarrollo de una aplicación compañera ("companion application"), o plataforma como un servicio. Otro ejemplo es la plataforma MS Office como servicio SaaS con su denominación de Microsoft Office 365, que incluye versiones online de la mayoría de las aplicaciones de esta suite ofimática de Microsoft.

Plataforma como servicio

La capa del medio, que es la plataforma como servicio (en inglés *platform as a service*, PaaS), es la encapsulación de una abstracción de un ambiente de desarrollo y el empaquetamiento de una carga de servicios. La carga arquetipo es una imagen Xen (parte de Servicios Web Amazon) conteniendo una pila básica Red (por ejemplo, un distro Linux, un servidor Red, y un ambiente de programación como Perl o Ruby). Las ofertas de PaaS pueden dar servicio a todas las fases del ciclo de desarrollo y pruebas del software, o pueden estar especializadas en cualquier área en particular, tal como la administración del contenido.

Los ejemplos comerciales incluyen Google App Engine, que sirve aplicaciones de la infraestructura Google, y también Windows Azure [2], de Microsoft, una plataforma en la nube que permite el desarrollo y ejecución de aplicaciones codificadas en varios lenguajes y tecnologías como .NET, Java y PHP. Servicios PaaS tales como éstos permiten gran flexibilidad, pero puede ser restringida por las capacidades que están disponibles a través del proveedor.

Infraestructura como servicio

La infraestructura como servicio (*infrastructure as a service*, IaaS) -también llamado en algunos casos hardware as a service, HaaS) se encuentra en la capa inferior y es un medio de entregar almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red. Servidores, sistemas de almacenamiento, conexiones, enrutadores, y otros sistemas se concentran (por ejemplo a través de la tecnología de virtualización) para manejar tipos específicos de cargas de trabajo —desde procesamiento en lotes ("batch") hasta aumento de servidor/almacenamiento durante las cargas pico. El ejemplo comercial mejor conocido es Amazon Web Services, cuyos servicios EC2 y S3 ofrecen cómputo y servicios de almacenamiento esenciales (respectivamente). Otro ejemplo es Joyent cuyo producto principal es una línea de servidores virtualizados, que proveen una infraestructura en-demanda altamente escalable para manejar sitios Web, incluyendo aplicaciones Web complejas escritas en Ruby en Rails, PHP, Python, y Java.

Tipos de nubes

- Las nubes públicas se manejan por terceras partes, y los trabajos de muchos clientes diferentes pueden estar mezclados en los servidores, los sistemas de almacenamiento y otras infraestructuras de la nube. Los usuarios finales no conocen qué trabajos de otros clientes pueden estar corriendo en el mismo servidor, red, discos como los suyos propios.

- Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. Las nubes privadas están en una infraestructura en-demanda manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.

- Las nubes híbridas combinan los modelos de nubes públicas y privadas. Usted es propietario de unas partes y comparte otras, aunque de una manera controlada. Las nubes híbridas ofrecen la promesa del escalado aprovisionada externamente, en-demanda, pero añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Las empresas pueden sentir cierta atracción por la promesa de una nube híbrida, pero esta opción, al menos inicialmente, estará probablemente reservada a aplicaciones simples sin condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas.

Comparaciones

La computación en nube usualmente es confundida con la computación en *grid* (red) (una forma de computación distribuida por la que "un súper computador virtual" está compuesto de un conjunto ó cluster enlazado de ordenadores débilmente acoplados, actuando en concierto para realizar tareas muy grandes).[8]

Controversia

Dado que la computación en nube no permite a los usuarios poseer físicamente los dispositivos de almacenamiento de sus datos (con la excepción de la posibilidad de copiar los datos a un dispositivo de almacenamiento externo, como una unidad flash USB o un disco duro), deja la responsabilidad del almacenamiento de datos y su control en manos del proveedor.

La computación en nube ha sido criticada por limitar la libertad de los usuarios y hacerlos dependientes del proveedor de servicios. Algunos críticos afirman que sólo es posible usar las aplicaciones y servicios que el proveedor esté dispuesto a ofrecer. Así, *The Times* compara la computación en nube con los sistemas centralizados de los años 50 y 60, en los que los usuarios se conectaban a través de terminales "gregarios" con ordenadores centrales. Generalmente, los usuarios no tenían libertad para instalar nuevas aplicaciones, y necesitaban la aprobación de administradores para desempeñar determinadas tareas. En suma, se limitaba tanto la libertad como la creatividad. El *Times* argumenta que la computación en nube es un retorno a esa época y numerosos expertos respaldan la teoría.[10]

De forma similar, Richard Stallman, fundador de la Free Software Foundation, cree que la computación en nube pone en peligro las libertades de los usuarios, porque éstos dejan su privacidad y datos personales en manos de terceros. Ha afirmado que la computación en nube es "*simplemente una trampa destinada a obligar a más gente a adquirir sistemas propietarios, bloqueados, que les costarán más y más conforme pase el tiempo.*"

Aplicaciones

- iCloud - desarrollado por Apple Inc.
- Campaign Cloud - desarrollado por ElectionMall.Com powerd by Microsoft
- Dropbox - desarrollado por Dropbox
- Google Docs - Desarrollado por Google

Cloud Computing: ¿Por qué no arranca?

Por Andrés Mutti, profesor de la carrera Ingeniería en Informática, de UADE

Cloud Computing es un nuevo paradigma, joven y en pleno desarrollo, que está dominando el escenario tecnológico actual para las empresas en el ámbito internacional. Sin embargo, a pesar del gran impulso que local e internacionalmente le están dando empresas como Google, Microsoft, IBM, CISCO, Hewlett Packard y VMware, entre otras, y sin dejar de lado a las telcos y los ISP locales, en el ámbito nacional su penetración es bastante más tímida -o precavida-.

En estos últimos días se realizó la primera jornada de TICs Argentina 2011, organizado por CICOMRA (Cámara de Informática y Comunicaciones de la República Argentina) y Reed Exhibitions, en la que el tema de los negocios en la nube fue relevante. En este sentido, las empresas argentinas no tienen aún un

porcentaje significativo de aporte al crecimiento de este nuevo paradigma o, al menos, a la par de otros países.

Antes de tratar de analizar la problemática del por qué las empresas argentinas no alientan el crecimiento del Cloud Computing, deberíamos puntualizar algunas definiciones acerca de la nube, dado que, justamente, la nube es vista muy bien desde afuera pero en su interior todo resulta nebuloso. Esto se debe, en parte, a que existen demasiados términos que reflejan la gran variedad de servicios que se pueden manejar y obtener desde la nube. Pero no todos son de fácil comprensión para el usuario no especializado en esta tecnología y -por qué no decirlo- a veces también para los profesionales entendidos, no especializados, existen algunos puntos borrosos.

Los conceptos

Veamos algunos ejemplos: términos como SaaS (software como servicio, por sus siglas en inglés) donde el cliente utiliza el software y las aplicaciones instaladas en la nube; IaaS (infraestructura como servicio), en la que el cliente accede a una infraestructura de servidores y/o equipos virtuales que se hallan en la nube; o el PaaS (plataforma como servicio), por medio del cual se accede a una plataforma con el fin de desarrollar nuevos productos. También nos encontramos con términos como public cloud (nube pública) y private cloud (nube privada), donde el primero no es más que un modelo por medio del cual el proveedor ofrece bajo el estándar de cloud computing servicios ya preparados de aplicaciones o storage. Éstos se pueden ofrecer en forma gratuita -como lo hacen Google Docs, Windows Live y Sky Drive entre otros-, o pay-per-usage, versión paga de los recursos que se usan - como Office 365, Microsoft Online Services y Windows Azure Platform, entre otros-. Las principales ventajas de este modelo son su muy bajo costo y la velocidad de puesta en marcha, ya que el costo del hardware, aplicaciones y ancho de banda corren por cuenta del proveedor; también tienen gran escalabilidad (bajo demanda) y el no desperdicio de recursos, puesto que se paga por lo que se usa (en el último caso).

El segundo término, private cloud, también denominado nube interna o nube corporativa, es usado para definir una arquitectura propietaria que utiliza técnicas de cloud y presta servicios de hosting a un reducido número de usuarios a través de un firewall. De esta manera, las empresas logran tener un control mayor sobre su información, aunque a un costo bastante más elevado respecto del public cloud. Como decíamos y mostramos, toda esta terminología y mucha otra, aunque parezca sencilla, esconde una complejidad técnica muy importante. Desconocer el significado que implican éstos y otros términos, promueve dudas, complicaciones -y hasta errores- que entorpecen la toma de una decisión, haciendo que ésta, incluso, pueda verse postergada.

Más poder

No obstante, es innegable que este nuevo paradigma dotaría a las empresas de mayor poder de computación, software actualizado, bajos costos de mantenimiento, portabilidad (dado que los datos o aplicaciones están en Internet y se puede acceder a ellos desde cualquier lugar), rápida puesta en marcha, y la seguridad y privacidad de la información.

Este último punto -la seguridad y privacidad de la información- es, tal vez, el más discutible del paradigma y el que acaso haga dudar más a los empresarios en apostar por un cambio a esta tecnología. Sin dudas, esta situación se ve alentada por el hecho de que cada día se descubren nuevas vulnerabilidades y brechas de seguridad dentro de la estructura informática de las empresas. Y teniendo en cuenta que estos entornos son más controlados y predecibles que la nube, es dable suponer, entonces, que en la nube podría haber todavía peligros y/o técnicas de acechanza que aún no son conocidos o predecibles… Un riesgo que muchos no están dispuestos a afrontar.

Además de lo mencionado, hay que tener en cuenta que la mayor parte de las empresas nacionales están o bien finalizando o bien en medio de los procesos de consolidación de servidores comenzados hace unos años, por lo que todavía no están dispuestas a producir un nuevo cambio en su estructura informática. Asimismo, las herramientas de gestión de procesos y de automatización con que cuentan actualmente en su mayor parte no están preparadas para realizar la misma función en la nube.

Seguridad y privacidad son aspectos neurálgicos para cualquier empresa. Habida cuenta de que todo esto acarrearía, además, un elevado costo inicial de puesta en marcha, creo comprender la reticencia de las empresas argentinas a apostar a la nube.