Sistemas informáticos multiusuarios y en red

Indice

1. Introducción a la informática

Introducción a la informática

Se conoce con el nombre de **Telecomunicaciones** a la disciplina que se encarga de estudiar los métodos y tecnologías para la transmisión de información. Con las redes de ordenadores surge una nueva disciplina, llamada **Telemática**, que bebe de ambas y se encarga de estudiar el ordenador como medio de comunicación.

La disciplina de la informática nace con la intención de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo y de gestión, donde es frecuente la repetición de tareas.

La **informática** es la disciplina que estudia el tratamiento automático y racional de la información.

En dicho lugar hace su aparición el vocablo **INFORMATIQUE**, procedente de la contracción de las palabras francesas **INFOR**mation auto**MATIQUE**. Dicho vocablo fue posteriormente reconocido y adoptado por el resto de países. Más concretamente, en España, el vocablo fue admitido en 1.968 bajo el nombre de **INFORMÁTICA**, que como se puede deducir fácilmente, es producto de la contracción de las palabras castellanas **INFOR**mación auto**MÁTICA**. En los países anglosajones, por su parte, a esta disciplina se la conoce con el nombre de **Computer Science**.

Elementos y conceptos básicos

El ordenador es una máquina compuesta de elementos físicos, en su mayoría de origen electrónico, capaz de realizar una gran variedad de trabajos a gran velocidad y con gran precisión, siempre que se le den las instrucciones adecuadas.

El conjunto de órdenes que se dan a un ordenador para realizar un proceso determinado se denomina **programa**.

El conjunto de uno o varios programas, más la documentación correspondiente para realizar un determinado trabajo, se denomina **aplicación informática**.

El **ordenador** es una máquina digital capaz de resolver cualquier problema que esté especificado mediante una serie de instrucciones (programa).

Un **sistema informático** se define como el **sistema compuesto de equipos y de personal** pertinente, que realiza funciones de entrada, proceso, almacenamiento, salida y control, con el fin de llevar a cabo una secuencia de operaciones con datos.

Hardware es la parte física del ordenador mientras que **software** es la parte lógica.

Concepto de información

Se define **información** como el conjunto de símbolos que representan algún hecho, concepto u objeto del mundo real. Por otra parte, llamamos **datos** al conjunto de expresiones que denotan valores, magnitudes, condiciones, estados, etc. El ordenador trabaja exclusivamente con datos y que somos nosotros, las personas, los que al interpretar dichos datos extraemos la información que llevan asociada.

Las **instrucciones** informan al ordenador sobre las operaciones a realizar, el modo de ejecutarlas, los medios y datos a emplear y sobre los que operar, el tiempo de la ejecución, etc.

Sistemas de información

Para que exista transmisión de información son necesarios tres elementos: emisor, receptor y medio.

Una vez que la información está en el interior del ordenador se puede empezar a actuar sobre la misma, realizando las transformaciones que sean necesarias para la consecución del objetivo que se persiga. Al conjunto de operaciones que se realizan sobre una información se le denomina **tratamiento de la información**.

Se denomina **entrada** al conjunto de operaciones cuya misión es **tomar los datos del exterior**, del medio, **y depositarlos en el interior del ordenador**; para ello, en ocasiones es necesario realizar operaciones de **depuración o validación** de los mismos.

Al **conjunto de operaciones** que se elaboran sobre los datos de entrada para obtener los resultados o datos de salida se le llama **proceso** o **algorítmo**.

Por último, se denomina **salida** al conjunto de operaciones que proporcionan los **resultados.**

Generaciones de ordenadores

- **Primera Generación**. viene marcado por la aparición del UNIVAC-I, en 1951. Los ordenadores eran máquinas **grandes y pesadas**, que ocupaban habitaciones completas. Se programaba en lenguaje máquina. El ordenador se limitaba a los campos científicos y militares.
- **Segunda Generación:** Podemos fechar el comienzo de la segunda generación en el año 1958, con la aparición del transistor. En esta época los ordenadores comienzan a utilizar **circuitostransistorizados** (con transistores), cuyo **consumo eléctrico** es bastante **inferior** al de las válvulas electrónicas. El ordenador es el IBM 1401. Para programar se utilizaba lenguaje ensamblador y lenguajes de alto nivel **Fortran, Cobol y Algol**. El ordenador se extiende a campos de administración y gestión.
- **Tercera Generación:** En 1964, la aparición del IBM-360, marca el nacimiento de la tercera generación de ordenadores. Llegan los **circuitos intergrados y los chips**. Se programa con **lenguajes de alto nivel, como Basic, Pascal y PL/1.**
- **Cuarta Generación**. La cuarta generación de ordenadores da comienzo a principios de los años 70, muchos hablan de solo una variante de la tercera. Se caracteriza por la aparición del **microchip**. El primer ordenador personal en EEUU fue el Altair 8800 de la empresa MITS construido en 1974.
- **Quinta Generación.** A finales de los 70 y llega hasta nuestros días. Viene marcada por la aparición del **microprocesador**.

Las información y su representación interna

Los ordenadores, debido a su construcción, solamente pueden trabajar en **forma binaria**. Un ordenador está compuesto de circuitos electrónicos sobre los cuales sólo se puede evaluar si hay o no hay corriente; por lo tanto, sólo se reconocen **dos estados o valores: 0 y 1.** Sin embargo el ordenador para comunicarse con nosotros usa numeración octal, decimal o hexadecimal.
Definimos **sistema de numeración** como el conjunto de símbolos y reglas que se utilizan para

representar cantidades o datos numéricos.

Sistema decimal

- Es uno de los **sistemas** denominados **posicionales** pues utiliza un **conjunto de símbolos cuyo significado o valor depende de su posición relativa al punto decimal**.
- La **base** de este sistema de numeración es **10.**
- Los **símbolos o cifras** que utiliza el sistema decimal son los siguientes: **0 1 2 3 4 5 6 7 8 9**.

Con n cifras decimales se pueden representar 10^n números, los que van del 0 al 10^n - 1.

Sistema binario

- La **base** de este sistema de numeración es **2.**
- Los símbolos o cifras que se utilizan para la representación: **0 1**.
- Cada cifra o dígito de un número representado en este sistema se denomina **bit**, que es la menor unidad de información posible en un ordenador.

Con n cifras binarias se pueden representar 2^n números, los que van del 0 al 2^n - 1.

Sistema Octal

El sistema octal, al igual que el sistema decimal y el sistema binario, es un sistema de numeración de los llamados posicionales cuya base es 8 y que, por tanto, utiliza ocho símbolos o cifras distintas para componer sus números: 0 1 2 3 4 5 6 7.

Sistema Hexadecimal

El sistema hexadecimal, al igual que los sistemas anteriores, es un sistema de numeración posicional, cuya **base** es **16** y que utiliza las siguientes **cifras** o **símbolos** para componer sus números: **0 1 2 3 4 5 6 7 8 9 A B C D E F**.

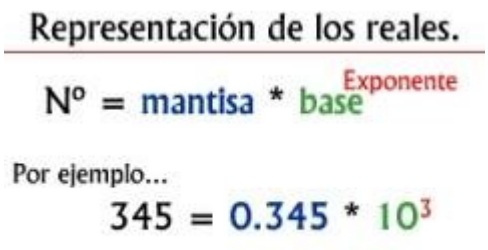
Representación interna de los números enteros

De principio tenemos los **número enteros** que corresponden a todos los números, negativos y positivos. Después los **números naturales,** que en términos informáticos se llaman **enteros sin signo**. Los ordenadores suelen usar una capacidad de **32 bits** para almacenar los números enteros, aunque es algo que depende de la arquitectura del propio procesador. Para representar los números enteros usaremos los 32 bits (binarios) para representarlos. Para representar los número naturales usaremos la representación **signo-magnitud**, que consiste en que el primer número representa el signo (0 para positivos y 1 para negativos) y los 31 bits restantes el número.

Representación interna de los números reales

Para representar los números reales el ordenador utiliza lo que se conoce con el nombre de **representación en punto flotante**. Para ello necesitamos 3 campos:

- **1 bit de signo**, que será 0 si el número es positivo y 1 si es negativo.
- **Exponente**. Recoge la codificación del número que hace de exponente en la notación científica.
- **Mantisa**. la codificación del número después del 0' de la notación científica.



La utilizamos para representar números reales y enteros mayores que los representables como números enteros

Codificación alfanumérica

- **Caracteres alfabéticos**: letras maýusculas y minúsculas sin la Ñ
- **Decimales:** tratados como caracteres
- **Caracteres especiales**: como punto, coma, asterisco y órdenes de control que sirven para mandarle al ordenador alguna instrucción.

Para la representación de información alfanumérica se utiliza lo que se conoce con el nombre de código. Un **código** no es más que una tabla de equivalencia en la que a cada carácter o símbolo que se quiere representar se le asigna un número binario.

Los primeros era código de 6 bits (64 caracteres), que almacenaban las letras minúculas y números. Luego llegaron los códigos de 7 bits (128 caracteres) que representaban las máyusculas también y caracteres con órdenes de control entre periféricos, el **código ASCII.**

Hoy en día los códigos más utilizados son el ASCII extendido, de 8 bits, y UNICODE, de 16 bits y de amplio uso en Internet y el mundo de las redes en general.

Estructura interna del ordenador

La **estructura física básica de un sistema informático** está compuesta de cuatro elementos:

- La **Unidad Central de Proceso (CPU**), o elemento ejecutor de las instrucciones de programas.
- La **memoria principal o central,** o elemento en el que tienen que estar ubicados los programas para que éstos puedan ser ejecutados por la CPU.
- Los **periféricos**, o unidades externas que permiten a la CPU comunicarse con el mundo exterior.
- Los **buses**, o canales de comunicación que unen los distintos componentes para hacer posible la comunicación entre ellos.

La Unidad Central de Proceso (CPU)

Haciendo una analogía, podríamos establecer que la CPU es tanto el **cerebro** como el **corazón** de la máquina. Es el elemento que sabe qué es lo que hay que hacer en cada momento y sabe qué órdenes hay que dar al resto de elementos para que la tarea se lleve a cabo. La CPU es la encargada de **controlar los periféricos, la memoria y la información** que se va a procesar. También es el elemento que **marca el ritmo de funcionamiento.** También se le llama **procesador.** Está formada físicamente por unos **circuitos electrónicos integrados en un solo chip**, llamado **microprocesador**.

Podemos establecerle que las siguientes funciones:

- **Funciones de Proceso**. Es decir, la CPU tiene la misión de ejecutar las instrucciones que forman los programas, realizando para ello los cálculos aritméticos y lógicos que sean necesarios.
- **Funciones de Control**. Es decir, supervisar todas las operaciones del sistema informático, controlando el flujo de datos entre los distintos elementos, y controlar que todo el sistema funciona correctamente.

Elementos internos de la CPU

- **Unidad de Control (UC):** Es el componente que controla el funcionamiento de la CPU y, por consiguiente, del ordenador. Entre las **funciones principales** de la Unidad de Control están la de encargase de **extraer o capturar las instrucciones del programa que se tienen que ejecutar**, la de encargarse de **analizar o decodificar las instrucciones para poder ejecutarlas** y la de **emitir las órdenes necesarias al resto de elementos del procesador para la ejecución de las instrucciones**.
- **Unidad aritmético-lógica** (ALU, de las siglas inglesas). Es el **componente que se encarga de realizar las operaciones aritméticas**, es decir, los cálculos (sumas, restas, etc.), **y las operaciones lógicas**, es decir, las comparaciones.
- **Registros del procesador:** Los registros del procesador son zonas de almacenamiento o memoria, en un principio de 16 bits, actualmente de 32 y muy pronto de 64. La ALU sólo puede operar sobre los registros, por lo que antes de poder operar con ningún dato que se encuentre en la **memoria principal del sistema**, la **CPU deberá primero traerlo** desde allí hacia alguno de sus registros. Estos registros que se usan para almacenar datos antes de ser operados o datos resultado de alguna operación se llaman **registros de datos** o **registros de propósito general**. También existe un registro especial, y muy importante, que recibe el nombre de **registro Contador de Programa**. Este registro se encarga de almacenar la dirección de memoria donde se encuentra almacenada la siguiente instrucción a ejecutar.

El procesador también tiene un **reloj** que marca la **velocidad de proceso** o **frecuencia o ciclo de reloj a la que trabaja**. Cualquier operación no puede durar menos de un ciclo de reloj, aunque sí puede suceder que dure varios ciclos de reloj. La unidad de medida de la frecuencia es el **Hertzio o Hercio**, que indica el número de ciclos de reloj que hay en 1 segundo.

La memoria principal

La misión de toda memoria, sea cual sea su tipo, es la de **almacenar información**. En el caso de la memoria principal, **su misión es la de almacenar los programas que se encuentran en ejecución, así como los datos que utilizan dichos programas**. Para que un programa se pueda ejecutar tiene que estar en **memoria central o principal**, pues es la **única memoria**

accesible o direccionable directamente por el procesador.
Podemos encontrar dos tipos de memoria distinta:

- **Memoria ROM:** que es una memoria de sólo lectura.
- **Memoria RAM:** que es una memoria en la que se puede tanto leer como escribir.

Podemos ver la memoria principal como un armario con distintos casilleros o **celdillas de memoria**, cada uno de los cuales tiene un identificador, número o **dirección**, y en cada uno de los cuales se puede guardar o **almacenar** un papel o **información**. Para acceder a las celdillas de memoria, el procesador tiene que atender al concepto de **dirección de memoria.**

Periféricos

Los periféricos tienen la misión de relacionar la CPU con el mundo exterior. Existen tres:

- **Periféricos de entrada**
- **Periféricos de salida**
- **Periféricos de entrada-salida**

La CPU se comunica con los periféricos a través de unas direcciones especiales que no se refieren a celdas de memoria sino a dichos periféricos. Dichas direcciones especiales reciben el nombre de **puertos**. Cuando son los periféricos los que necesitan comunicarse con la CPU, deben provocar lo que se llama una **interrupción,** para que la CPU, que es la única unidad capaz de procesar información, deje lo que estuviese haciendo y atienda al periférico para hacer lo que éste necesite.

Buses

La CPU se comunica con los pereféricos a través de unas líneas eléctricas que sirven para transmitir información entre los distintos componentes del ordenador y que se llaman **buses**. Existen los siguientes tipos de buses:

- **Bus de datos**. Llevan información de datos desde y hacia la CPU, por lo que se dice que son bidireccionales.
- **Bus de direcciones**. Permiten al microprocesador seleccionar una de las tantas posiciones de memoria, ya sea para lectura o escritura. Se dice que es unidireccional, pues tan sólo es el procesador el que puede poner información en este bus, el resto de elementos del sistema tan sólo puede leerlo.
- **Bus de control**. Son buses que permiten al microprocesador sincronizarse con los distintos dispositivos para efectuar la transferencia de información entre ellos.

2. Introducción a los periféricos

Introducción a los pereféricos

Se pueden clasificar los periféricos en:

- **Periféricos internos.** Son los que se encuentran dentro de la **carcasa del ordenador.** Estas ranuras se comunican directamente con unos buses de la placa que se llaman, consecuentemente, **buses de expansión**.
- **Periféricos externos.** Son los que se encuentran fuera de la carcasa del ordenador y se conectan a él a través de los **puertos**,
- **Periféricos integrados en placa.** Son los que se encuentran dentro de la carcasa del ordenador pero forman parte de la propia **placa base**, no pudiendo ser separados de ésta.

Buses y tarjetas de expansión

Los periféricos internos podrían conectarse directamente al **bus de sistema.** Sin embargo, una solución mejor consiste en conectarlos a un bus adicional, llamado **bus de expansión**. Esta disposición permite:

- conectar al sistema una amplia variedad de dispositivos periféricos
- aislar el tráfico de información entre la memoria y el procesador, del tráfico correspondiente a la Entrada/Salida.

Este bus adicional se encontrará comunicado con el bus de sistema a través de un dispositivos llamado "**interfaz del bus de expansión**", cuya misión es la de regular las transferencias de datos entre el bus de sistema y los controladores conectados a dicho bus de expansión.

Principales buses de expansión:

- **Bus ISA.** Bus de expansión con una **anchura de bus** de **16 bits** y con una **frecuencia de funcionamiento** de hasta **8 Mhz** . En un principio recibía el nombre de bus AT. Es un bus de expansión ya obsoleto y suelen ser de color negro.

- **Bus PCI.** Bus de expansión de alto rendimiento con una **anchura de bus** de **32 bits**, **bus PCI convencional**, o **64 bits, bus PCI - X**, con **frecuencias de funcionamiento** de **33 Mhz** para las primeras y de **66 Mhz o 133 Mhz** para las segundas. **Las ranuras de expansión PCI suelen ser de color blanco crema y suele haber unas 4 o 5 en la placa**.

  Entre las principales aportaciones de PCI es su **capacidad Plug&Play.** Este tipo de tarjetas vienen provistas de un chip de memoria ROM en el que viene guardada toda la información necesaria para el proceso de configuración.

- **Bus AGP.** Con la aparición de necesidades de tratamiento masivo y más rápido de gráficos 2D y 3D, se han tenido que mejorar de alguna manera las prestaciones que ofrece el bus PCI a las **tarjetas gráficas**. Es un nuevo estándar diseñado por Intel y que ha sido acogido por la gran totalidad de empresas que se dedican a fabricar tarjetas de vídeo o chips de aceleración gráfica. El bus AGP proporciona una **vía de comunicación ultrarrápida entre el sistema de memoria principal y el controlador gráfico**, además, al situar en él la tarjeta gráfica, que es probablemente el periférico que más tráfico genere, el **bus PCI queda más descargado, mejorándose el rendimiento global del sistema**. El bus AGP sólo soporta una ranura de expansión; es decir, este bus se utilizará

exclusivamente para vídeo. Dicha ranura de expansión suele ser de **color marrón**.

Recientemente, con el auge de los ordenadores portátiles, se han popularizado mucho unas tarjetas de expansión del tamaño de las tarjetas de crédito, llamadas **tarjetas PCMCIA.** Las tarjetas de expansión que sigan el estándar PCMCIA tendrán capacidad Plug&Play y capacidad de conexión en caliente, con lo que para instalarlas y poder usarlas sólo habrá que introducirlas en el tarjetero PCMCIA.

Conectores externos

La mayoría de las placas base de los ordenadores incorporan conectores, que suelen recibir el nombre de puertos, como los siguientes:

- **Conector o puerto serie.** Este tipo de conector recibe este nombre porque sirve para instalar **dispositivos serie** (dispositivo que trasmite los datos bit a bit). Una placa base, por sí misma, es capaz de reconocer hasta cuatro conectores serie, aunque lo normal es que los ordenadores traigan sólo dos. Estos conectores reciben el nombre de **COMx** (si hay dos conectores, COM1 y COM2) o conectores RS232. Los hay de 2 tipos: los de **9 pines** y los de **25 pines**. Para estos dispositivos, la placa proporciona el conector macho, mientras que los periféricos proporcionan el conector hembra. Los conectores serie de 25 pines se dejaron de montar con la aparición de los Pentium, por lo que podemos considerarlos obsoletos
- **Conector o puerto paralelo.** Este tipo de conector recibe este nombre porque sirve para instalar **dispositivos paralelos**. Los conectores paralelos son de **25 pines**, hembra en la placa y macho en el dispositivo. A estos conectores se les denomina **LPTx**. Los periféricos paralelos más importantes son la impresora y algunos tipos de escáner.
- **Conector o puerto PS/2:** Algunos ratones antiguos se conectan al puerto serie; sin embargo, actualmente, el conector más habitual para este tipo de dispositivos es el llamado PS/2, en el cual también es posible conectar los teclados. También recibe el nombre de mini-DIN, evolución de un conector más antiguo, llamado conector DIN.
    - **Conector DIN.** Su función es la de **conectar el teclado exclusivamente**. El conector en la placa es hembra de cinco pines en forma circular. Con el nacimiento del **mini-DIN** ha dejado de tener importancia y ya no viene en las placas modernas.
    - **Conector mini-DIN o PS/2.** Su función es admitir **periféricos como el ratón o el teclado**. Muy similar al del conector DIN pero mucho más pequeño. Normalmente, un ordenador integra dos conectores de este tipo, uno para el **ratón (verde)** y otro para el **teclado (violeta)**
- **Conector o puerto USB:** El conector USB (Universal Serial Bus - **Bus Serie Universal**) nace como un estándar de entrada/salida de velocidad media-alta. A través de un conector USB se pueden conectar en cadena hasta un total de 127 periféricos. Cuenta con capacidad PnP (Plug and Play) y la facilidad de conexión "en caliente". Tres características:
    - **Dos velocidades de acceso**, una baja de **1,5 Mbps** para dispositivos lentos, como pueden ser joysticks o teclados, y otra alta, de **12 Mbps**, para los dispositivos que necesiten mayor ancho de banda.
    - **Topología en estrella**, lo que implica la necesidad de dispositivos tipo "**hub**" que centralicen las conexiones
    - **Permite suministrar energía eléctrica a dispositivos** que no tengan un alto consumo y que no estén a más de 5 metros

  Existen dos **especificaciones USB**: la **V1.1** (12 Mb/s) y la **V2.0** (260 y 480 Mb/s), que se diferencian principalmente en la **tasa de transferencia.** Además, son compatibles hacia

atrás, un dispositivo 2.0 funciona en un 1.1

El teclado

Los primeros modelos tenían 83 teclas y no incluían indicadores luminosos de ningún tipo. Son conocidos como teclados PC/XT, ya que sólo pueden utilizarse en ordenadores de tipo XT. Más tarde surgió el teclado AT, que ya disponía de indicadores luminosos.

Tras éste apareció el AT extendido, que básicamente ya no se ha cambiado. Éste consta de 101 teclas (102 en los modelos internacionales, en el caso de España para la "ñ") entre las que se encuentran una serie de teclas suplementarias utilizadas para emitir órdenes hacia la unidad central o para facilitar el uso de programas. Los cambios que ha sufrido este periférico están relacionados con la **ergonomía**

Atendiendo a la manera en la que hacen contacto sus teclas, existen básicamente dos tipos de teclados: los **teclados de contacto mecánico** y los **teclados de contacto capacitivo o de membrana.**

Recientemente han irrumpido con fuerza en el mercado los **teclados inalámbricos**, cuya principal particularidad es que carecen de cables.

El ratón

Podemos clasificar los ratones en: ratones mecánicos y ópticos. Existe otro periférico llamado **Trackball**, que no es más que un ratón al revés, de forma que el usuario mueve directamente la bola con el dedo pulgar sin tener que mover el ratón.

El escaner

El escáner es el **periférico de entrada** que sirve para introducir (**digitalizar**) en el ordenador dibujos, fotografías, gráficos, etc., que se encuentran en papel. Los hay de mesa y de mano.

El monitor

Periférico de salida mas importante. El tamaño de los monitores se mide en pulgadas y lo que se mide es la longitud de la diagonal del mismo. Otra característica importante en un monitor es la resolución, que se define como el número de pixeles que puede representar el monitor en la pantalla.

Atendiendo a la tecnología que utilizan, se distinguen dos tipos principales de monitores, los monitores **CRT** y los monitores o pantallas **LCD**.

- **El monitor CRT:** Los monitores más utilizados en la actualidad son los monitores de tubo de rayos catódicos o monitores CRT. Para que una imagen se vea en pantalla es necesario iluminar absolutamente todos los píxeles que la componen; es decir, encender todos los píxeles de la pantalla. Para conseguir esto en los monitores CRT, es preciso realizar un barrido de pantalla, el cual se realiza por líneas horizontales de izquierda a derecha y de arriba abajo. Una vez realizado el barrido comienza el siguiente. Esta acción

recibe el nombre de refresco de la imagen.

La velocidad o **frecuencia de refresco**, o **frecuencia vertical**, de un monitor hace referencia al número de veces que se dibuja la pantalla por segundo. Esta velocidad se mide en Hertzios (Hz), donde un Hertzio indica un barrido completo de la pantalla por segundo. Está estimado que a partir de 85 Hz para no percibir parpadeo, y que 70 o 75 Hz es una frecuencia de refresco aceptable. El mínimo son 60 Hz, por debajo de esta cifra los ojos sufrendemasiado. Algunos monitores CRT utilizan una técnica llamada **entrelazado**, consistente en que la pantalla se dibuja en dos pasadas, primero las líneas impares y luego las pares. Es recomendable utilizar un monitor no entrelazado. Por otra parte, se conoce como **frecuencia horizontal** al número de veces por segundo que el haz de electrones debe desplazarse de izquierda a derecha de la pantalla.

- **El monitor LCD:** Otro tipo de pantallas son las de cristal líquido, lamadas también **LCD** (Liquid Cristal Display), que son **delgadas pantallas planas de gran resolución y calidad**

  Dentro de la gama de monitores LCD existentes, están los de **matriz pasiva** (pantallas **DSTN** - Dual Scan Twisted Nematic) y los de **matriz activa** (pantallas **TFT** - Thin Film Transistor), cuya diferencia radica en la distinta manera que tienen de aplicar corriente a las celdas de cristal líquido.

Compativa:

- Un monitor LCD pesa menos y ocupa mucho menos espacio que un monitor CRT
- Un monitor LCD consume mucha menos energía que un monitor CRT.
- Un monitor CRT es bastante más barato que un monitor LCD.
- El parpadeo en las pantallas LCD queda sumamente reducido por el hecho de que cada celda donde se alojan los cristales líquidos está encendida o apagada, de modo que la imagen no necesita una renovación (refresco).
- En los monitores LCD, al no producirse un bombardeo de electrones, sino que simplemente interviene la luz, no emiten radiaciones electromagnéticas dañinas.
- Los monitores CRT tienen mejor ángulo de visión. En un monitor LCD es necesario estar situado enfrente de la pantalla, pues si estás un poco desplazado, no verás la imagen correctamente.
- Los monitores CRT pueden presentar una mayor gama de colores así como conseguir una mayor pureza del color.

Impresoras

Podemos distinguir tres **categorías de impresoras:**

- **Matricial:** El cabezal de estas impresoras está formado por una matriz de puntos. Asociado a cada punto hay una aguja. Para cada carácter se activan las agujas adecuadas y se hace incidir el cabezal sobre una cinta con tinta, y ésta sobre el papel. Los caracteres se forman como un conjunto de puntos. Estas impresoras son las únicas que permiten obtener varias copias simultáneas de un mismo impreso mediante el uso de papel autocopiado (calco) de varias hojas.
  La velocidad se mide en cps o caracteres por segundo. La calidad, normalmente, viene marcada por el número de agujas, que suelen oscilar entre las 8 y las 24, siendo mejor cuanto de mayor número disponga. Elevado ruido y su poca definición. Podemos

considerar su economía, tanto en compra como en mantenimiento.

- **Impresora de inyección de tinta (inkjet):** Su funcionamiento se basa en la expulsión de gotas de tinta líquida a través de unos inyectores que impactan en el papel formando los puntos necesarios para la realización de gráficos y textos. La velocidad, que se mide en **páginas por minuto** (ppm), y que suele ser distinta dependiendo de si imprimimos en color o en monocromo, y la **resolución máxima**, que se mide en ppp o puntos por pulgada (dpi en inglés).
- **Impresora láser.** El material que se utiliza para la impresión es un polvo muy fino que pasa a un rodillo que, previamente magnetizado en las zonas que contendrán la parte impresa, es pasado a muy alta temperatura por encima del papel, que por acción de dicho calor, se funde y lo impregna. Estas impresoras suelen ser utilizadas en el mundo empresarial, ya que su precio de coste es más alto que el de las de inyección de tinta, pero su coste de mantenimiento es más bajo. Una de las características más importantes de estas impresoras es que pueden llegar a **velocidades muy altas**, medidas en **páginas por minuto** o ppm. Su resolución también puede ser muy elevada y su **calidad muy alta**

Dispositivos y soportes de memoria secundaria

Los ordenadores tienen una **memoria interna** que usan intensivamente para almacenar los datos y los resultados más inmediatos.

- Esta memoria tiene un tiempo de acceso muy pequeño y, por tanto, el ordenador opera con ella rápidamente.
- Tiene una capacidad limitada
- Para evitar esta limitación, se usa la memoria auxiliar externa o memoria secundaria, que es de acceso lento (comparada con la memoria interna) pero de gran capacidad.

Según la **tecnología que utilizan para almacenar y leer la información**, los dispositivos y soportes de almacenamiento secundario se pueden clasificar en:

- **Dispositivos y soportes magnéticos.** Son aquéllos que para almacenar la información utilizan las propiedades magnéticas de los elementos que lo componen. En este tipo de soportes existe una película de plástico recubierta de una fina superficie de algún elemento magnéticamente sensible, como hierro o cromo, que en un principio se encuentra disperso según un patrón aleatorio.
- **Dispositivos y soportes ópticos**. Son aquéllos que, para almacenar la información, se basan en la propiedad de reflexión de la luz.

Por otra parte, **según la manera de acceder a la información almacenada**, se diferencian:

- **Dispositivos y soportes de acceso secuencial.** Son aquéllos en los que el paso de una posición de memoria a otra requiere transitar por toda la información intermedia.
- **Dispositivos y soportes de acceso directo.** Son aquéllos en los que se puede ir de una zona del disco a otra directamente

Tipos de dispositivos:

- **La unidad de cinta y las cintas magnéticas:** Caracteristicas:
    - Memoria de lectura/escritura y no volátil
    - La cinta se mueve delante de las cabezas lectoras/escritoras, existiendo contacto físico entre la cinta y éstas.
    - El soporte es muy económico.

    - El acceso es puramente secuencial, tiempo de acceso muy elevado
    - No se puede intercalar información adicional.

- **La disquetera y los disquetes magnéticos:** El disquete magnético es un soporte liviano, removible y portable: se extrae y se puede transportar a cualquier sitio. Según su tamaño:
    - Discos de 5 y 1/4.
    - Discos de 3 y 1/2.

  Parámetros a considerar:
    - Densidad de grabación: es el número de bits que se graban por pulgada (bpi, bits per inch.).
    - Densidad de pistas: mide el número de pistas por pulgada de longitud (tpi, tracks per inch).
    - Capacidad de almacenamiento: es el número de bits que pueden almacenarse en el disco.

  Los elementos principales son:
    - Motor de arrastre. Está controlado por un circuito electrónico que mantiene la velocidad de giro dentro de unos límites estrechos.
    - Motor de posicionamiento. El motor de posicionamiento del cabezal es un motor que arrastra el brazo del cabezal sobre las pistas del disquete.
    - Cabezal magnético. Es de reducidas dimensiones y efectúa las operaciones de lectura/escritura.

  Algunos parámetros son:
    - Velocidad de rotación: se mide en rpm (revoluciones por minuto) y suele ser de 300 rpm.
    - Tiempo de acceso: Tiempo que pasa desde que la información es solicitada al periférico hasta que el cabezal de lectura del mismo puede leer la información del sector en el que se encuentra almacenada dicha información.
    - Velocidad de transferencia: es la velocidad medida en Mbytes/segundo a que los datos son transmitidos a la CPU del computador, y viene dada por la velocidad de rotación y por la densidad de grabación.

- **El disco duro:** periférico y soporte de información van juntos, formando un todo, a diferencia con el diskete. Varios discos de material magnético montados sobre un eje central sobre el que giran. En cuanto al formato físico del disco, siguen existiendo los conceptos de pista y sector, pero aparece uno nuevo: el concepto de cilindro. Un cilindro está formado por el conjunto de pistas que ocupan la misma posición en cada uno de los discos.

  Los elementos principales:
    - Eje. Es la parte del disco duro que actúa como soporte, sobre el cual están montados y giran los platos. Equivalente a motor de arrastres de la disketera.
    - Peine. También llamado impulsor de cabezas o brazo, es el mecanismo que mueve las cabezas de lectura/escritura radial a través de la superficie de los platos de la unidad de disco
    - Cabezas de lectura/escritura. Es la parte de la unidad de disco que escribe y lee los datos del disco.

  La velocidad de rotación en los discos duros es mucho mayor que en los disquetes, así como existe mayor densidad de pista. Además, en los discos duros no existe contacto físico entre el cabezal de lectura/escritura y la superficie del disco.

  Los parámetros son:
    - Capacidad.
    - Velocidad de rotación. varían entre los 5.400 rpm de las gamas medias o los 7.200 e incluso 10.000 de los mejores productos

    - Caché. Los discos duros también hacen uso de unos almacenes temporales de datos para acceder a la información más frecuente de forma mucho más veloz.
    - Interfaz. La interfaz es la conexión entre el mecanismo de la unidad de disco y el bus del sistema y define la forma en que las señales pasan entre el bus del sistema y el disco duro. Es el canal de comunicación sobre el que fluyen los datos leídos y escritos al disco duro. La interfaz del disco duro es como un dispositivo más conectado al bus de expansión. Hay dos tipos: IDE y SCSI

- **El disco ZIP y la unidad ZIP:** una capacidad de 100 MB y 250 MB. Sus buenas prestaciones se deben a su alta velocidad de rotación, de 3.000 rpm y su buffer de 256 KB para hacer más rápido el acceso. Esta unidad existe en formato externo e interno, con conexiones SCSI (tanto interno como externo), IDE (sólo interno), puerto paralelo y puerto USB.

- **El CD y el lector/grabador de CDs.** Estos soportes de información y sus respectivos periféricos pertenecen ya a los que utilizan tecnología óptica para almacenar la información. Distinguimos los siguientes tipos de CDs:
    - El CD-ROM. Son unidades de sólo lectura
    - El CD-R. El CD-R (Recordable) o disco compacto grabable es un disco que puede ser grabado por el usuario una sola vez y, una vez grabado, se convierte en un dispositivo de sólo lectura.
    - El CD-RW. El CD-RW (Rewritable) o disco compacto regrabable es un soporte óptico de lectura en el cual la grabación produce cambios físicos en el medio, pero estos cambios son reversibles por la naturaleza de los materiales que se usan para la fabricación de los CDs.

- **El DVD y el lector/grabador de DVDs.** La principal diferencia es la capacidad de almacenamiento. Se ha reducido y compactado el tramado de puntos que se asientan sobre la superficie del disco y que pueden ser adulterados para reflejar o no el haz láser. Es necesario un láser mucho más preciso. Al igual que ocurre con los CDs, podemos hablar de DVD-ROM, DVD-Recordable y DVD-Regrabable

- **Los lápices o llaveros de memoria Flash:** Estos llaveros de memoria se conectan al puerto USB y se basan en el uso de memoria ROM de tipo Flash para almacenar la información,

3. Software de un sistema informático

Sofware de un sistema informático

Se puede clasificar el software:

- **Sistema operativo:** Es un software que permite administrar los recursos del ordenador. Los recursos son: la memoria, el procesador, los dispositivos de entrada/salida, los dispositivos de comunicación y datos y los medios de almacenamiento masivo. En realidad el sistema operativo no **es un solo programa**, sino que lo forman una gran variedad de estos, cada uno tiene una misión asignada y todos juntos hacen que el ordenador funcione, también hace de **interfaz** entre el hardware y el resto de software que utilizamos. También proporciona una **interfaz de línea de comandos** o una **interfaz gráfica** al usuario, para que este último se pueda **comunicar con el ordenador**.
- **Programas de aplicación:** Es el software que **se superpone al sistema operativo** y se aprovecha de él para proporcionarnos las diferentes funcionalidades que le vamos a pedir a nuestro sistema informático.

Sistema operativo

Su función no es otra que hacer de **enlace entre el hardware** de nuestra máquina y los **programas de aplicación** que utilicemos.

El sistema operativo es:

- los programas que hacen utilizable el hardware
- son ante todo administradores de recursos; el principal recurso que administran es el hardware del ordenador.
- actúa como intermediario entre el usuario y el hardware del ordenador y su propósito es proporcionar el entorno en el cual el usuario pueda ejecutar programas.
- Un sistema operativo es un conjunto de programas que controla la ejecución de programas de aplicación y actúa como una interfaz entre el usuario y el hardware de un ordenador.

Las características deseables de un sistema operativo son:

- **Eficiencia**: Un sistema operativo permite que los recursos del ordenador se usen de la manera más eficiente posible.
- **Fiabilidad:** Un sistema operativo no debe tener errores y debe prever todas las posibles situaciones críticas y resolverlas si es que se producen.
- **Robustez:** El sistema operativo debe responder de forma predecible y controlada a

condiciones de error, incluidos fallos hardware.
- **Seguridad:** El sistema operativo debe protegerse activamente a sí mismo y a los usuarios de acciones accidentales o malintencionadas.
- **Extensibilidad:** La aparición constante de nuevo hardware y de nuevos tipos de aplicaciones, exigen al sistema operativo la adición de nueva funcionalidad.
- **Facilitar las entradas y salidas**: Un sistema operativo debe hacerle fácil al usuario el acceso y manejo de los dispositivos de Entrada/Salida del ordenador.
- **Manejar las comunicaciones en red:** El sistema operativo debe permitir al usuario manejar con alta facilidad todo lo referente a la instalación y uso de las redes de ordenadores
- **Permitir a los usuarios compartir recursos y datos**: Este aspecto está muy relacionado con el anterior y daría al sistema operativo el papel de regulador de los recursos de una red.
- **Disponer de un entorno amigable y de fácil uso**

Evolución histórica

Se puede decir que la **evolución de los sistemas operativos va paralela a la evolución de los ordenadores** donde se ejecutan.

- **Primera Generación (años 50):** Los primeros sistemas operativos eran muy básicos y rudimentarios. Surgieron en los años cincuenta, con los primeros ordenadores de tubos de vacío. Estos primeros sistemas operativos se limitaban a controlar y secuenciar la ejecución de programas y sus datos, que en aquella época estaban escritos en tarjetas perforadas. Las **tarjetas perforadas** llevaban escritas las instrucciones de programa en forma de agujeros en una cartulina, que una máquina lectora de tarjetas comunicaba al sistema operativo.
- **Segunda Generación (años 60):** Aparecen los **ordenadores construidos a base de transistores**, cada vez más pequeños y potentes.
- **Tercera Generación (años 70):** la introducción en la industria del **circuito integrado** que sustituía a los transistores provocó que de nuevo se buscaran técnicas para mejorar el rendimiento y así aparece el concepto de **multiprogramación** (en un mismo procesador, de varios programas a la vez). Para ello se emplea el **tiempo compartido** (*time sharing*) en el que a través de políticas de asignación
- **Cuarta Generación (años 80 a nuestros días):** están ligadas a los **avances en la industria del hardware.** Ya no sólo se trata de incrementar la velocidad de los procesos, sino de aumentar la **seguridad** y las **prestaciones.** Hay sistemas que controlan lo que se denomina **proceso distribuido**, consistente en la **conexión en paralelo de varios ordenadores** compartiendo memoria, buses y terminales con el fin de ganar seguridad en el servicio. Para incrementar la velocidad de proceso, existe el **multiproceso**, consistente en **ordenadores que poseen más de un procesador.** Aparecen sistemas operativos en red para controlar el trabajo que se realiza en una red de ordenadores

Sistemas Operativos clasificados por su estructura. Se entiende por estructura del sistema operativo a la forma como se divide internamente y cuáles son las relaciones entre las distintas partes.

- **Estructura monolítica: Un sólo programa con un conjunto de rutinas.**

  Es la estructura de los primeros sistemas operativos constituidos fundamentalmente por un solo programa compuesto de un conjunto de rutinas entrelazadas de tal forma que cada una puede llamar a cualquier otra.

- **Estructura jerárquica: Organizado en niveles.**
  Es donde una parte del sistema contiene subpartes y está organizado en forma de niveles, de tal forma que cada una de ellos esté perfectamente definido y con una clara interface con el resto de elementos. En esta estructura se basan prácticamente la mayoría de los sistemas operativos actuales.
- **Máquina Virtual: Multiprogramación y máquina extendida**
  Se trata de un tipo de sistemas operativos que presentan una interface a cada proceso, mostrando una máquina que parece idéntica a la máquina real subyacente. Estos sistemas operativos separan dos conceptos que suelen estar unidos en el resto de sistemas: la multiprogramación y la máquina extendida. El objetivo de los sistemas operativos de máquina virtual es el de integrar distintos sistemas operativos dando la sensación de ser varias máquinas diferentes.
- **Microkernel o micronúcleo: Aumenta la portabilidad entre plataformas**
  Se conoce como microkernel al modelo de kernel (núcleo) de sistema operativo, que consiste en distribuir las diferentes tareas en porciones de código modulares y sencillas. Se pretende aislar del sistema, su núcleo, las operaciones de entrada/salida, gestión de memoria, etc., que se realizarían en procesos separados. Esto mejora la tolerancia a fallos y eleva la portabilidad entre plataformas de hardware. Algunos sistemas que utilizan esta tecnología son AIX, MACOSX o Hurd.

Sistemas Operativos clasificados por sus servicios.

Por el número de usuarios simultáneos que soporta

- **Monousuario:** Soportan un único usuario a la vez, sin importar el número de procesadores que tenga el ordenador o el número de procesos o tareas que pueda ejecutar en un mismo instante de tiempo (MS-DOS, Windows 3.1, 95, 98 y Millenium)
- **Multiusuario:** Son capaces de dar servicio a uno o más usuarios a la vez, ya sea por medio de varias terminales conectadas al ordenador o por medio de accesos remotos en una red de comunicaciones. (UNIX, Linux, NETWARE, Windows NT, Windows 2000 Server, LAN Manager (IBM))

Por el número de tareas (trabajos) que pueden ejecutar al mismo tiempo

- **Monotarea:** Permiten realizar una sola tarea a la vez por usuario.
- **Multitarea:** Soportan la ejecución de dos o más trabajos activos al mismo tiempo. (UNIX, Windows 95, 98, NT, 2000, MAC-OS, OS/2.)

Por el número de procesos simultáneos

- **Uniproceso:** Es capaz de manejar solo un proceso del ordenador simultáneamente. (MS-DOS y Windows 95, 98, Millenium y XP)
- **Multiproceso:** Estos pueden ser simétricos o asimétricos y se necesita que el hardware del ordenador tenga varios procesadores. El sistema gestionará su utilización administrará la carga de trabajo de cada uno. (UNIX, Linux o Windows 2000 y 2003 Server)

Procesos

Un proceso en un programa en ejecución. Un proceso simple tiene un hilo de ejecución. La diferencia entre un programa y un proceso:

- un proceso es una actividad de cierto tipo que contiene un programa; entradas, salidas y estados.
- un programa está compuesto por procesos.

Un proceso puede estar en cualquiera de los siguientes tres estados:

- **Listo:** son los que pueden pasar a estado de ejecución si el planificador del sistema operativo los selecciona
- **En ejecución:** son los que se están ejecutando en el procesador en un momento dado.
- **Bloqueado:** están esperando la respuesta de algún otro proceso para poder continuar con su ejecución

Los procesos pueden:

- Cooperar: los procesos interactúan entre sí y pertenecen a una misma aplicación
- Ser independientes: no interactúan y un proceso no requiere información de otros

La planificación del procesador se refiere a la manera o técnicas que se usan para decidir cuánto tiempo de ejecución se le asigna a cada proceso del sistema y en qué momento. Para lograr la implementación del modelo de procesos el sistema operativo almacena en una tabla denominada **tabla de control de procesos** la información relativa a cada proceso que se esta ejecutando en el procesador. La información que se almacena es la siguiente:

1. Identificación del proceso.
2. Identificación del proceso padre.
3. Información sobre el usuario y grupo. Que lo han lanzado.
4. Estado del procesador. El contenido de los registros internos, contador de programa, etc. Es decir el entorno volátil del proceso.
5. Información de control de proceso
6. Información del planificador.
7. Segmentos de memoria asignados.
8. Recursos asignados.

Una **estrategia de planificación** debe buscar que los procesos obtengan sus turnos de ejecución de forma apropiada, junto con un buen rendimiento y minimización de la sobrecarga (overhead) del planificador mismo. Se buscan **cinco objetivos principales**:

1. Justicia o Imparcialidad
2. **Maximizar la Producción**: El sistema debe **finalizar el mayor número de procesos** por unidad tiempo.
3. **Maximizar el Tiempo de Respuesta**:
4. **Evitar el aplazamiento indefinido**: Los **procesos deben terminar en un plazo finito de tiempo**.
5. **El sistema debe ser predecible**: Ante cargas de trabajo ligeras el sistema debe responder rápido y con cargas pesadas debe ir degradándose paulatinamente.

Características a considerar de los procesos:

1. Cantidad de Entrada/Salida: Existen procesos que realizan una gran cantidad de operaciones de entrada y salida (aplicaciones de bases de datos, por ejemplo).
2. Cantidad de Uso de CPU: Existen procesos que no realizan muchas operaciones de

entrada y salida, sino que usan intensivamente la unidad central de procesamiento. Por ejemplo, operaciones con matrices y cálculos matemáticos.

3. Procesos por lotes frente a procesos interactivos: Un proceso por lotes es más eficiente en cuanto a la lectura de datos, ya que generalmente lo hace de archivos, mientras que un programa interactivo espera mucho tiempo (no es lo mismo el tiempo de lectura de un archivo que la velocidad en que una persona teclea datos) por las respuestas de los usuarios.
4. Procesos en Tiempo Real: Si los procesos deben dar respuesta en tiempo real se requiere que tengan prioridad para los turnos de ejecución.
5. Longevidad de los Procesos: Existen procesos que típicamente requerirán varias horas para finalizar su labor, mientras que existen otros que solo necesitan algunos segundos.

La planificación apropiativa (preemptive) es aquélla en la cual, una vez que a un proceso le toca su turno de ejecución ya no puede ser suspendido. **La planificación no apropiativa (not preemptive)** es aquélla en que existe un reloj que lanza interrupciones periódicas en las cuales el planificador toma el control y se decide si el mismo proceso seguirá ejecutándose o se le da su turno a otro proceso.

Los algoritmos para determinar el orden de ejecución de los procesos en el sistema en la planificación no apropiada son:

- **Round Robin:** También llamada por turno, consiste en darle a cada proceso un intervalo de tiempo de ejecución (llamado time slice), y cada vez que se vence ese intervalo se copia el contexto del proceso a un lugar seguro y se le da su turno a otro proceso. Los procesos están ordenados en una cola circular.
- **Por prioridad:** Los procesos de mayor prioridad se ejecutan primero. Si existen varios procesos de mayor prioridad que otros, pero entre ellos con la misma prioridad, pueden ejecutarse estos de acuerdo a su orden de llegada o por 'round robin'. La ventaja de este algoritmo es que es flexible en cuanto a permitir que ciertos procesos se ejecuten primero e, incluso, por más tiempo. Su desventaja es que puede provocar aplazamiento indefinido en los procesos de baja prioridad.
- **El trabajo más corto primero:** Es difícil de llevar a cabo porque se requiere saber o tener una estimación de cuánto tiempo necesita el proceso para terminar. Pero si se sabe, se ejecutan primero aquellos trabajos que necesitan menos tiempo y de esta manera se obtiene el mejor tiempo de respuesta promedio para todos los procesos.
- **El primero en llegar, primero en ejecutarse:** Es muy simple, los procesos reciben su turno conforme llegan. La ventaja de este algoritmo es que es justo y no provoca aplazamiento indefinido. La desventaja es que no aprovecha ninguna característica de los procesos y puede no servir para un proceso de tiempo real.
- **El tiempo restante más corto:** Es parecido al del trabajo más corto primero, pero aquí se está calculando en todo momento cuánto tiempo le resta para terminar a todos los procesos, incluyendo los nuevos, y aquel que le quede menos tiempo para finalizar es escogido para ejecutarse.
- **La tasa de respuesta más alta:** Este algoritmo concede el turno de ejecución al proceso que produzca el valor mayor de la siguiente formula:

$$\text{VALOR} = \frac{\text{Tiempo que ha esperado} + \text{Tiempo Total para terminar}}{\text{Tiempo Total para terminar}}$$

Gestión de la memoria

Si se pretende que un proceso pueda ejecutarse es necesario que éste sea cargado en memoria principal, ya que ningún proceso se puede activar antes de que se le asigne el espacio de memoria que requiere. La memoria será otro recurso que el sistema operativo tendrá que gestionar y el elemento que se encargará de ello recibe el nombre de **gestor de memoria.**

La misión del gestor de memoria es la de asignar memoria principal a los procesos que la soliciten. Entre otras cosas tendrá que:

- llevar el control de las zonas que están en uso y cuáles no,
- asignar memoria a los procesos cuando la necesiten y retirársela cuando terminen,
- tendrá que establecer mecanismos para que un proceso no invada la memoria asignada a otro proceso,
- administrar el intercambio entre memoria principal y memoria secundaria cuando la memoria central sea insuficiente, etc.

Sus objetivos son:

- **Reubicación:** Consiste en decidir en qué zona de la memoria se ubicará un proceso y cómo se gestionará la posibilidad de que un proceso cambie de zona de memoria asignada.
- **Control de memoria:** tiene que llevar un control de las zonas de memoria libres y de las zonas de memoria asignadas, así como conocer a qué proceso pertenece cada una de las zonas de memoria. Proporcionen memoria a los procesos que lo necesiten y se la retire cuando éstos hayan terminado.
- **Protección:** El sistema operativo tiene que conseguir que la zona de memoria asignada a un proceso no sea accedida ni alterada por los demás.
- **Utilización de dos niveles de memoria:** tendrá que proporcionar los medios para trabajar con una memoria secundaria y tendrá que encargarse de gestionar la transferencia de información entre la memoria principal y la secundaria.

Gestión de memoria en sistemas operativos monotarea

El esquema más sencillo de gestión de memoria es aquél en el que, en cada instante, sólo se tiene un proceso en memoria. En este esquema hace falta un mecanismo de protección para que resulte imposible el acceso a la zona de memoria destinada al sistema operativo por parte del proceso de usuario que se esté ejecutando.

Gestión de memoria en sistemas operativos multitarea

Todos estos procesos deberán estar también simultáneamente en memoria, pues ésta es una condición necesaria para que un proceso pueda ejecutarse. Por tanto, deberá haber mecanismos de gestión para distribuir la memoria principal entre todos estos procesos que quieren ejecutarse.

- **Intercambio o swapping:** puede suceder que haya más procesos de los que caben en memoria y no haya memoria principal disponible para todos. En esos casos algunos de esos procesos se almacenan en disco, para posteriormente recuperarlos. El intercambio o swapping hace referencia a las operaciones de eliminar de la memoria principal procesos suspendidos, llevarlos al disco y cargar del disco a memoria principal procesos para su

ejecución. La memoria en disco que el sistema operativo reserva para almacenar estos procesos suspendidos recibe el nombre de **espacio de intercambio o espacio de swapping** y siempre va a almacenar procesos completos que se han retirado completamente de memoria.

- **Asignación con particiones fijas:** La gestión de la memoria con particiones fijas supone que la división de ésta se ha realizado con anterioridad al comienzo de la ejecución de los procesos. Las particiones, una vez hechas por el sistema operativo, se mantienen fijas tanto en número como en tamaño. La forma de gestión se puede resumir:

    1. Cuando llega una tarea, ésta se pone en una **cola de tareas**.
    2. El **intercambiador** tiene en cuenta los requerimientos de memoria de cada una de ellas y las particiones disponibles.
    3. Si una tarea tiene espacio disponible en memoria, **se ubica (o reubica) en una partición y puede competir por el uso de la CPU**.
    4. Cuando se termina una tarea, **se libera la partición de memoria** que ocupa, pudiendo el intercambiador asignar esta partición a otra tarea de la cola de tareas.

    La gestión y asignación de particiones a los procesos se puede hacer siguiendo dos tipos de organización:

    1. **Tener una cola por partición.** Se tiene **una cola por cada partición** y se coloca cada trabajo en la cola de la partición más pequeña en que quepa dicho trabajo, a fin de desperdiciar el menor espacio posible.
    2. **Tener una única cola común a todas las particiones.**

    En los dos casos tendrá que haber **mecanismos para proteger a un proceso de los demás.** Otro problema que aparece cuando se gestiona la memoria con particiones fijas es el de la **fragmentación**, la cual se produce, en general, cuando en la memoria hay áreas ocupadas intercaladas con áreas libres; es decir, cuando no hay una única área ocupada ni una única área libre.

- **Asignación con particiones variables:** permite que los tamaños de las particiones varíen dinámicamente. Se consigue un mejor uso de la memoria aunque a costa de una mayor complejidad. **El procedimiento que se sigue para manejar y gestionar la memoria** es el siguiente:

    1. Cuando **llega un proceso y precisa memoria** se busca un hueco libre suficientemente grande para él. Si se encuentra uno, **se le asigna sólo la memoria que sea necesaria**, manteniendo el resto disponible para satisfacer futuras solicitudes.
    2. Cuando un proceso acaba, **libera su bloque de memoria**, que se devuelve entonces al conjunto de huecos. Si el nuevo hueco es adyacente a otros, se fusionan para formar un hueco mayor.

Paginación

La **fragmentación externa** se produce cuando la memoria disponible no es contigua. Este problema tiene como solución la **paginación**, que es un **mecanismo de organización y asignaciónde la memoria** que permite que la memoria asignada a un proceso no tenga por qué ser contigua, de forma que siempre que se disponga de espacio, aunque éste no sea adyacente, se pueda asignar al proceso.

En un sistema de memoria con paginación, la memoria física se divide:

- un número de **bloques de tamaños fijos**, denominados **marcos de página**.

- Por otra parte, el espacio de direcciones lógico de un proceso (es decir, **todas las posibles direcciones que puede generar el proceso**) también se divide en bloques de tamaño fijo, llamados **páginas**, que son del mismo tamaño que los marcos de página.

Memoria Virtual

La idea de permitir la ejecución de procesos que puedan no estar cargados completamente en memoria, e incluso que sus tamaños superen a la memoria física disponible, da lugar al concepto de memoria virtual.

4. Software de un sistema informático (II)

Gestión de entrada/salida

El sistema operativo hace que los dispositivos se conecten al sistema y realicen sus funciones de forma controlada y eficiente. El sistema operativo debe perseguir que los programas sean independientes de los dispositivos y actúa de intermediario entre ellos.

Es imposible hacer un programa de aplicación que contemple toda la extensa gama de dispositivos diferentes que se pueden encontrar. En lugar de esto lo que se hace es estandarizar el acceso a los dispositivos utilizando lo que se llaman controladores de dispositivos (*device drivers*). Estos controladores actúan como **interface entre los programas y el hardware.** Cada vez que conectemos físicamente un **nuevo dispositivo** a un ordenador deberemos paralelamente **instalar la conexión lógica de dicho dispositivo**, que no es otra que el **controlador**.

Existen tres tipos de métodos de funcionamiento de un controlador, según sea el tipo de intervención de la CPU en el proceso.

- **Entrada/salida programada:** En este caso la **CPU lleva todo el peso de la operación** de entrada/salida. También se conoce como **entrada/salida por sondeo o *polling***. La CPU "pregunta" directamente al dispositivo si tiene algún dato para enviar o está listo para recibir datos, si es así se inicia el proceso con total control por parte de la CPU. Este método **tiene el inconveniente de repercutir en la velocidad de proceso del ordenador** porque la CPU debe dejar todo lo que está haciendo para ocuparse del proceso de entrada/salida.
- **Entrada/salida por interrupciones:** Habría que introducir el concepto de interrupción: es un mecanismo **por el cual se avisa a la CPU que debe dejar lo que esté haciendo** (interrumpir su trabajo) para atender al dispositivo. En este caso no es la CPU quien pregunta (sondeo o *polling*) sino que **es el propio dispositivo de entrada/salida el que interrumpe a la CPU** sólo cuando hace falta. Gana en velocidad respecto al anterior
- **Acceso directo a memoria:** Existe un **método todavía más eficiente** que consiste en **liberar totalmente a la CPU** en el proceso. También llamado **DMA**. Lo habitual es que los datos que se quieren escribir en el dispositivo o que son leídos del dispositivo provengan o vayan a la memoria del ordenador, pues bien en este caso la CPU inicia el proceso, pero luego este continúa sin necesitar a la CPU, con lo que **se acelera mucho el proceso de entrada/salida**. Para realizar este tipo de transferencia se utiliza un circuito integrado (*chip*) especialmente diseñado para este fin.

Existen unas estructuras de datos que se utilizan para permitir la comunicación fluida entre dispositivos o entre dispositivos y CPU. Las más importantes son los ***spools*** y los ***buffers*.**

- ***Spools*:** Una técnica muy común, especialmente en salida, es el uso de "*spoolers*". Los datos de salida se almacenan de forma temporal en una cola situada en un dispositivo de almacenamiento masivo (*spool*), hasta que el dispositivo periférico requerido se encuentre libre. De este modo se evita que un programa quede retenido porque el periférico no esté disponible. El sistema operativo dispone de llamadas para añadir y eliminar archivos del *spool*. Se utiliza cuando el dispositivo necesita todos los datos de salida de golpe antes de iniciar su tarea. Por ejemplo una impresora no puede empezar a imprimir si no tiene el fichero que se quiere imprimir entero. Se utiliza en dispositivos que no admiten intercalación, como ocurre en la impresora. Puesto que en este caso cuando se empieza a imprimir un trabajo no puede empezar con otro hasta que no ha terminado.

- ***Buffers*:** Es una técnica parecida al *spool,* pero en este caso se utiliza para dispositivos que admiten intercalación, es decir dispositivos que pueden atender peticiones de distintos orígenes. En este caso los datos no tienen que enviarse completos, pueden enviarse porciones que el *buffer* retiene de forma temporal. También se utilizan para acoplar velocidades de distintos dispositivos. Por ejemplo si un dispositivo lento va a recibir información que le llega más rápido de lo que puede atender se utiliza un *buffer* para retener de forma temporal la información hasta que el dispositivo se desahoga un poco, es el caso de una grabadora de CD (lenta) en comparación con la velocidad que el disco duro le envía datos.

Algoritmos para gestionar las peticiones de acceso a disco:

- **Algoritmo FCFS (First Come, First Served). Primero en llegar, primero en ser servido**

  Esta planificación hará uso de una cola tipo FIFO. Es inherentemente justo. Sin embargo, en promedio, puede dar lugar a tiempos bastante grandes.

- **Algoritmo SSF (Shortest Seek First). Primero la búsqueda más cercana**

  Atiende primero la solicitud de la cola de solicitudes pendientes que quiere acceder al cilindro más cercano al de la solicitud actual, que se está procesando. Requiere el menor movimiento de la cabeza de lectura/escritura. Es un algoritmo bastante habitual. Un **inconveniente** es que pueden llegar solicitudes que impliquen cilindros próximos al actual y serán atendidos enseguida mientras que otras que llegaron antesno se atenderán. Esta situación se conoce con el nombre de **bloqueo indefinido**. Tampoco es un algoritmo óptimo (no garantiza que la secuencia elegida sea la mejor)

- **Algoritmo Scan o algoritmo del ascensor.**

  Va dando servicio a las solicitudes que van encontrando en el sentido en el que se van desplazando las cabezas de lectura/escritura. Cuando no hay más solicitudes en ese sentido, o se llega al extremo, se invierte el sentido para hacer lo mismo otra vez pero yendo hacia el otro lado. Es necesario tener un bit que indique el sentido del movimiento. Evita el bloqueo indefinido. La cuota máxima del total de movimientos está fijada: es el doble del número de cilindros. Es más apropiado para sistemas que hacen gran uso del disco.

- **Algoritmo C-Scan o algoritmo Scan Circular.**

  Trata de evitar el problema anterior restringiendo el rastreo a una única dirección. En esta planificación la cabeza se mueve de un extremo del disco al otro, atendiendo las solicitudes que va encontrando, pero al llegar al extremo opuesto, regresa de inmediato al otro sin servir ninguna solicitud.

Sistema de archivos

Cada **sistema de archivos** (***file system***) utiliza métodos diferentes para llevar a cabo las operaciones de **almacenar, manipular, organizar, acceder y consultar los datos,** aunque por otra parte todos los sistemas de archivos tienen características comunes

Se puede definir un **sistema de archivos** como el **software** integrante del **sistema operativo** que proporciona **servicio a usuarios, aplicaciones y al propio sistema operativo** para utilizar archivos almacenados en disco.

Los objetivos que se persiguen al diseñar un sistema de archivos deben ser:

- **Acceso Rápido para recuperar la información contenida en archivos**:
- **Fácil actualización**:
- **Economía de almacenamiento**: Intentar que los archivos desperdicien la menor cantidad de espacio en disco posible
- **Mantenimiento simple**: Evitar las operaciones complicadas a usuarios y programas, ocultando los detalles y proporcionando un acceso estandarizado a los archivos.
- **Fiabilidad para asegurar la confianza en los datos:** Deben proveer sistemas que aseguren que los datos sean correctos y fiables y deben proveer características de recuperación de fallos o desastres
- **Incorporar mecanismos de seguridad y permisos**: Esto es especialmente importante en sistemas de archivos de sistemas operativos multiusuario.
- **Control de concurrencia**: Se debe controlar y asegurar el acceso correcto a los archivos por parte de varios usuarios a un tiempo, posiblemente bloqueando el archivo en uso hasta que termine la operación de modificación en curso.

Los sistemas de archivos deben proveer una capa de abstracción que oculte los detalles puramente hardware al usuario y le permita utilizar el medio de almacenamiento (disco) de una forma intuitiva y cómoda, por supuesto más cercana a los hábitos humanos de organización de la información. Éste es el nivel lógico del sistema de archivos y naturalmente en el que estamos más interesados.

A esto se le llama organización del sistema de archivos y suele coincidir en todos los sistemas de archivos actuales, utilizando el esquema de almacenamiento en archivos y la organización en carpetas o directorios.

Cada **archivo** de un sistema tendrá unas **características** que lo identifican y le sirven al sistema de archivos y al sistema operativo para manejarlo correctamente. A esas características se les llama **atributos** y aunque varían de un sistema a otro suelen coincidir al menos en las siguientes:

- **Nombre:** Cada sistema operativo establece las reglas para nombrar a los archivos, por ejemplo limitando la longitud del nombre en caracteres o prohibiendo el uso de algún carácter especial como parte del nombre. Incluso algunos sistemas diferencian entre nombres en mayúscula o minúscula.
- **Permisos:** El sistema de archivos debe llevar un registro de qué usuarios están autorizados a utilizar cada archivo y que operaciones pueden realizar.
- **Creador:** Identificador del usuario que creo el archivo.
- **Propietario:** Identificador del usuario que es el propietario actual del archivo.
- **Fecha de creación:** Fecha y hora de la creación del archivo.
- **Fecha del último acceso:** Fecha y hora del último acceso al archivo.
- **Fecha de la última modificación:** Fecha y hora de la última modificación al archivo.
- **Tamaño actual:** Número de bytes que ocupa el archivo en el disco duro del ordenador.

Directorios: También llamados **carpetas**, en realidad son archivos un poco especiales que almacenan información sobre la organización de los archivos y de otros directorios, **subdirectorios**.

En cuanto a los archivos las operaciones más comunes son:

- **Crear**: Los archivos se crean sin datos y después el usuario o alguna aplicación los van llenando.

- **Eliminar**: Si un archivo ya no es necesario debe eliminarse para liberar espacio en disco. Los sistemas operativos modernos utilizan el concepto de papelera de reciclaje para poder recuperar ficheros borrados accidentalmente.
- **Abrir**: Consiste en asignar un identificador a nivel de sistema operativo para poder referirse a él en las siguientes operaciones de lectura y escritura.
- **Cerrar**: Cuando concluyen los accesos, el identificador de archivo ya no es necesario.
- **Leer**: Los datos se leen del archivo; quien hace la llamada (programa) debe especificar la cantidad de datos necesarios y proporcionar un buffer para colocarlos.
- **Escribir**: Los datos se escriben en el archivo. El tamaño del archivo puede aumentar si se agregan datos nuevos o no si lo que se hace es actualizar los existentes.
- **Cambiar de nombre:** Permite modificar el atributo nombre de un archivo ya existente.

Operaciones más comunes con **directorios**:

- **Crear**: Se crea un directorio vacío.
- **Eliminar**: Se elimina un directorio, que debe estar vacío previamente. No se puede eliminar un directorio que contiene archivos o subdirectorios.
- **Abrir directorio**: Consiste en prepararlo para su uso. Por ejemplo, esta operación la hace el sistema de forma automática cuando se hace doble clic sobre una carpeta en el administrador de archivos.
- **Cerrar directorio**: Cuando se ha leído un directorio, éste debe ser cerrado.
- **Leer directorio**: Esta operación devuelve el contenido de un directorio en forma de lista de atributos de los archivos y subdirectorios que contiene.
- **Cambiar de nombre**: Cambia el nombre de un directorio de manera similar al cambio para archivos.

Los sistemas de archivos necesitan una forma de determinar la localización exacta de un archivo o directorio en la estructura del árbol de directorios. La técnica utilizada para ello consiste en nombrar todos los subdirectorios por donde hay que pasar para llegar al objetivo separados por algún carácter de separación (en Windows se utiliza la barra "\" y en Guadalinex y Linux se utiliza la barra "/"). A esto se le llama ruta de de acceso. Existen dos tipos de rutas de acceso:

1. Ruta de Acceso Absoluta: Consiste en empezar desde el directorio raíz e ir descendiendo en la estructura de directorios hasta llegar al archivo o directorio buscado.

2. Ruta de Acceso Relativa: Se utiliza junto con el concepto de directorio de trabajo o directorio activo, que es aquel donde estamos situados en un momento dado. Consiste en escribir la ruta a partir del directorio activo.

Existen muchos más tipos de sistemas de archivos.

- Sistemas Windows: Han evolucionado desde los sistemas FAT16 presente en MS-DOS, FAT32 utilizado por Windows 95/98 y NTFS utilizado por Windows 2000 y XP.
- Sistemas Linux: En la actualidad se utiliza Ext3, aunque antes existió Ext2. También es utilizado por algunas distribuciones Linux el sistema Reiser.

Protección y seguridad

- **La seguridad física** está muy relacionada con la figura del administrador del sistema,

puesto que es la persona encargada de diseñar los mecanismos para proporcionar seguridad al resto de los usuarios del sistema.
    - Asegurar el sistema contra desastres naturales como incendio, inundación, etc.
    - Asegurar el sistema contra accesos de personal no autorizado a los ordenadores y dispositivos.
    - Proveer medidas de recuperación fiables y rápidas ante roturas o averías de partes del sistema. Por ejemplo un SAI
- **Seguridad de acceso:** son mecanismos que garanticen la seguridad en cuanto a usuarios. El mecanismo fundamental en este punto es la utilización de contraseñas para acceder a los recursos del sistema y la gestión segura de las mismas. Por otra parte el sistema **de contraseñas debe ser lo suficientemente eficaz como para establecer niveles de acceso diferentes** o gestionar grupos de usuarios con intereses comunes.
- **Criptografía:** Se denomina criptografía al estudio de soluciones basadas en teorías matemáticas para cifrar y descifrar información. Se aplica en el cifrado de contraseñas o en el cifrado de datos para ser enviados por sistemas de comunicación susceptibles de ser interceptados. Técnicas:
    - **Criptografía simétrica:** En este caso se utiliza la misma clave para cifrar que para descifrar los mensajes. Tiene el inconveniente de que la clave la deben conocer las dos partes (la que cifra y la que descifra).
    - **Criptografía asimétrica:** Se utilizan claves diferentes para cifrar y para descifrar, lo que se conoce como sistema de claves pública/privada. Mejora los defectos del sistema simétrico.
- **Programas malignos:** consisten en programas diseñados con el ánimo de destruir o afectar a los sistemas informáticos. Son:
    - **Virus:** Consiste en un programa que tiene la **capacidad de copiarse a sí mismo** en otros programas "sanos" infectándolos y consiguiendo así su propagación (oculta al usuario). Actúa realizando alguna acción nociva para el sistema
    - **Gusano**: Es un tipo especial de virus que está diseñado para expandirseconsumiendo los recursos del ordenador hasta llegar a colapsarlo.
    - **Troyano**: Es un programa que infecta el ordenador victima sin darse a conocer y permite a una persona atacante del sistema en cuestión controlar sus funciones y robar datos, generalmente a través de Internet.
- **Copias de seguridad:** todo sistema cuente con aplicaciones diseñadas para realizar copias de seguridad (*backup*) y también se diseñe una planificación temporal para realizarlas. Existen varios métodos:
    - **Completa**: todo el sistema de archivos
    - **Incremental:** copia las variaciones de una copia completa anterior con respecto a la situación actual.

5. Redes (I)

Sistemas de comunicación

Llamamos **sistema de comunicación** al conjunto de dispositivos de cualquier naturaleza que colaboran con el único objetivo de hacer posible el intercambio de información entre dos entidades. Sus elementos son los siguientes:

- La **fuente** de la información. Es el dispositivo que genera los datos a transmitir.
- El **transmisor** de la información: elemento que necesita la fuente para transmitir.
- El **sistema de transmisión**. Es el sistema a través del cual viaja la información desde la fuente hacia el destino.
- El **receptor** de la información. elemento que necesita el destino para recibir la información
- El **destino** de la información. Es el dispositivo al que van dirigidos los datos transmitidos.

Esquema de conmutación

En las redes de comunicaciones existen principalmente dos **esquemas de conmutación**; es decir, dos filosofías para hacer llegar la información de la fuente al destino a través del sistema de transmisión. Estos dos mecanismos son:

- **La conmutación de circuitos:** Para que dos dispositivos puedan establecer una comunicación, primero establecen una ruta o circuito dedicado en exclusividad desde la fuente al origen, pasando por todos los nodos intermedios que sean necesarios. La comunicación se desarrolla en tres fases: conexión, transferencia y desconexión. Como toda la información sigue el mismo camino desde la fuente al destino, ésta llega en el orden en el que fue enviada. El ejemplo más significativo de uso de la conmutación de circuitos lo tenemos en la red telefónica.
- **La conmutación de paquetes:** Para transmitir datos a través de una red de este tipo, la información que se quiere transmitir se divide en trozos, llamados paquetes, que van siendo insertados en la red paulatinamente. Estos paquetes son encaminados o dirigidos a través de los nodos de la red, desde la fuente al destino, de manera independiente uno de otro; es decir, cada paquete puede seguir un camino distinto para llegar al destino y, por tanto, pueden llegar a él de manera desordenada. El destino tendrá, posteriormente, que ordenar y ensamblar de nuevo los distintos paquetes, conforme vayan llegando, para recomponer la información original. La mayor parte de las redes de transmisión de datos y las redes de ordenadores que utilizamos (Internet), usan este mecanismo de conmutación.

Red de ordenadores. Definición y ventajas

Una red de ordenadores es un conjunto de ordenadores autónomos (capacidad para funcionar por sí solos) y con capacidad de interconexión (posibilidad de intercambiar información). Cada uno de estos ordenadores conectados en red recibe el nombre de **host**.

La principal ventaja de las redes de ordenadores es la de poder intercambiar información entre los distintos equipos o hosts que forman parte de la misma. Derivadas de esta ventaja aparecen otras como las siguientes:

- **Ahorro económico**. Gracias a la posibilidad de compartir ciertos recursos, no es

necesario que cada ordenador tenga uno propio. Por ejemplo una impresora

- **Tolerancia a fallos**. En una red, ante el fallo de un recurso concreto puede utilizarse otro recurso disponible del mismo tipo sin ningún problema. Por ejemplo con dos impresoras, si falla una, tenemos la otra

- **Capacidad de crecimiento**. Las redes proporcionan gran flexibilidad para adaptar los recursos a las necesidades cambiantes de una empresa pues ofrecen la posibilidad de ampliar recursos de manera fácil y económica.

Protocolo de comunicación

Un **protocolo** es un acuerdo entre las partes que se comunican sobre cómo se va a proceder durante la comunicación para que ésta se pueda llevar a cabo de manera satisfactoria.

En el mundo de la comunicación por ordenador, llamaremos **Protocolo de comunicaciones** al conjunto de reglas que posibilitan que dos entidades puedan intercambiar información de manera ordenada y libre de errores.

Es momento de analizar el proceso que se debe seguir para diseñarlo. Para reducir la complejidad de su diseño, un protocolo de comunicación suele estar organizado como una serie de capas o niveles, cada una construida sobre la inferior y centrada en solucionar un problema concreto de la comunicación. A esta división en capas en las que se estructura un protocolo de comunicación se le llama **arquitectura** o **modelo del sistema de comunicación**. El objetivo que se persigue con esta estructuración en niveles o capas es la de simplificar el problema mediante su división en problemas más pequeños y más fácilmente abordables

Estructura en Capas

Cuando hay una estructuración en capas de un protocolo de comunicación, cada capa tiene la misión de resolver un problema concreto de la comunicación, para lo cual se responsabiliza de realizar unas determinadas tareas siguiendo sus propias reglas o protocolos para llevarlas a cabo. Además, cada capa ofrece una serie de servicios a la capa inmediatamente superior; es decir, le garantiza que sabe realizar la tarea que tiene encomendada, que sabe resolver el problema del que se encarga. **Cada capa conoce qué hace la capa inmediatamente inferior a ella, pero no tiene por qué saber cómo lo hace,** sólo conocen los servicios que le proporciona sin tener que preocuparse de cómo se llevan a cabo dichos servicios. Está totalmente abstraída de los problemas que le soluciona la capa inferior de la arquitectura.

En una red de ordenadores **es un conjunto de protocolos.** Al conjunto de protocolos empleados en un sistema o red de comunicaciones, estando cada uno de estos protocolos asociado a una capa concreta de dicho sistema, se le llama **pila de protocolos.**

Detallemos el proceso:

- En la **fuente de la comunicación** cada capa recibe datos de la capa **superior**. Estos datos son tratados de acuerdo a los protocolos establecidos en dicha capa y se añade a los mismos cierta **información de control** dirigida a la capa homóloga en el destino. Se dice entonces que **la capa n encapsula los datos de la capa n + 1**. El producto resultante es pasado a la capa inmediatamente inferior como datos de capa superior y el proceso se repite. Por tanto, conforme la información que se quiere enviar va bajando por la pila de protocolos, **cada capa va añadiendo su información de control a dicha información**.

- En el **destino de la comunicación** cada capa recibe datos de la capa **inferior**. Dichos datos incluyen tanto los datos de control que le pertenecen a la capa como los datos que tiene que enviar a la capa superior de la pila. Con la información de control que le pertenece, el protocolo de la capa puede realizar el trabajo que tiene encomendado. Entonces **desencapsula** los datos de la capa superior y se los envía a dicha capa, que repite el mismo proceso con los datos que le pertenecen. Por tanto, conforme los datos recibidos van ascendiendo por la pila de protocolos, **cada capa elimina su información de control**.

Este mecanismo de **encapsulación/desencapsulación** de información permite que **cada capa del dispositivo emisor se comunique virtualmente con la capa correspondiente (homóloga) del dispositivo receptor a través de la información de control que añade**. Se dice entonces que la capa n del dispositivo emisor se comunica con la capa *n* del dispositivo receptor mediante el protocolo de la capa *n*.

Una capa puede ofrecerle a la capa superior dos tipos de servicio:

- **Servicio orientado a la conexión.** Servicio en el que se garantiza que los datos le llegarán en orden a la capa homóloga del otro extremo de la comunicación, que no se producirán pérdidas de datos y que los datos llegarán sin errores.
- **Servicio no orientado a la conexión.** Servicio en el que los datos podrán llegar en cualquier orden a la capa homóloga del otro extremo de la comunicación, en el que no se garantiza que vayan a llegar sin errores, y en el que ni siquiera se garantiza la entrega de dichos datos; es decir, no se puede garantizar que los datos no se vayan a perder por el camino.

La pila de protocolos TCP/IP

En el mundo de las redes de ordenadores existen **dos protocolos de comunicación**: el **protocolo de comunicaciones OSI**, que es un protocolo que se ha quedado como modelo teórico (es decir, apenas se utiliza en el mundo real), y el **protocolo de comunicaciones TCP/IP**, que es el protocolo de comunicaciones más extendido en las redes de ordenadores y es el que se usa en el mundo Internet. El modelo TCP/IP divide la arquitectura de red en las siguientes capas o niveles:

- **Capa de acceso a red:** Todo host que forma parte de una red está conectado a ésta a través de un medio físico. Este nivel se encarga de abstraer al resto de todas las particularidades propias del medio físico al que se está conectando. Este nivel sería suficiente para hacer posible la comunicación entre hosts que comparten el mismo medio físico. De hecho, los hosts que se pueden comunicar directamente entre ellos a través del medio físico se dice que pertenecen a la misma red. El servicio que ofrece es el de hacer llegar la información a cualquier host de destino: **"dame la información que quieras que yo me comprometo a entregársela a tu capa homóloga de cualquier host que tú me digas, siempre y cuando dicho host pertenezca a la misma red que nosotros".**

- **Capa de interred (internet) o capa de red:** El nivel de interred o nivel de red se encarga de conectar dos host que no se encuentran en el mismo medio físico. Hace posible la comunicación entre hosts que se encuentran en redes distintas: **"dame la información que quieras que yo me comprometo a entregársela a tu capa homóloga de cualquier host que tu me digas, esté donde esté dicho host, en la misma red que nosotros o cualquier otra red interconectada".**

- **Capa de host a host o capa de transporte:** Una vez localizado dicho host es necesario saber con qué aplicación o proceso concreto dentro de ese host se quiere entablar la

comunicación, pues **hemos de tener presente que realmente no son dos ordenadores los que se comunican, sino dos aplicaciones o programas informáticos que se encuentran en ordenadores distintos** los que se comunican. Este nivel se centra en tratar los aspectos necesarios para que aplicaciones que se encuentran en hosts distintos de la red puedan entablar una comunicación. Asimismo, se encarga de ocultarle a las aplicaciones que tiene por encima la realidad de la red que tienen por debajo. Dichas aplicaciones se comunican pero no son conscientes de que se encuentran en ordenadores distintos: **"dame la información que quieras que yo me comprometo a entregársela a la aplicación que tú me digas del host que tú me digas, esté donde esté dicho host".**

- **Capa de proceso o capa de aplicación:** esta capa es donde se establecen las reglas que van a seguir dos aplicaciones para poder mantener una comunicación o un intercambio de información. A esta capa pertenecen los programas que proporcionan servicios de red como: servidores de correo (SMTP), servidores de transferencia de archivos (FTP), terminales remotos (Telnet), etc. Alguna de estas aplicaciones pueden interactuar con el usuario directamente mediante una interfaz, como por ejemplo las aplicaciones FTP y Telnet.

Capa de acceso a Red

En este nivel de la pila de protocolos tendrán que establecerse:

- los distintos **medios físicos** que se pueden utilizar para transmitir información,
- cómo se trabaja con cada uno de dichos medios físicos (es decir, cómo se **codifica y transmite** la información en cada uno de ellos),
- cómo tienen que ser los **dispositivos**, cables, clavijas, antenas... que se utilizarán para conectar el ordenador al medio físico,
- qué **problemas** o errores pueden aparecer en cada uno de los medios físicos y cómo se pueden evitar o solucionar dichos problemas o errores,
- cómo se van a **disponer** físicamente los distintos hosts,
- cómo se va a **coordinar** la comunicación entre dos equipos a través del mismo medio físico, etc.

Lo cual incluye básicamente dos aspectos:

- **Definición y especificación** de los medios físicos utilizables.
- **Coordinación de la comunicación** entre dos equipos a través de dicho medio físico, también llamado **enlace**.

Según el tipo de tecnología de transmisión que se utilice en el medio físico:

- **Redes de difusión**. Son aquéllas que tienen un solo canal de comunicación al que están conectadas todas las máquinas de la red. Es decir, son aquellas redes en las que el medio físico está compartido por todos los equipos que forman la red. Por ejemplo un profesor en una clase habla con un alumno, todos le oyen, pero sólo le escucha y atiende el alumno al que le habla

- **Redes punto a punto**: Son aquellas redes que están formadas por muchas conexiones entre pares individuales de máquinas. En este tipo de red, cuando una máquina quiere enviar una información a otra, ésta puede que tenga que visitar más de una máquina intermedia para poder llegar a su destino. Cada máquina tiene que tener información para ir encaminando la información y ésta puede seguir caminos diferentes para llegar de un mismo origen a un mismo destino.

Atendiendo a su **extensión geográfica**, las redes se pueden clasificar en:

- **Redes de Área Local (LAN - Local Area Network).** Se llama así a las redes que están dentro de un ámbito geográfico pequeño,

- **Redes de Área Extendida (WAN - Wide Area Network).** Se llama así a las redes que cubren una extensa área geográfica, como por ejemplo, un país, un continente, el planeta entero, etc.

- **Redes de Área Metropolitana (MAN - Metropolitan Area Network).** Recientemente, con la aparición de los operadores de cable, han aparecido redes que se encuentran a medio camino entre las redes de área local y las de área amplia. Dichas redes cubren el área geográfica de una ciudad.

El medio físico

Todo host que forma parte de una red está conectado a ésta mediante un medio físico. La manera en la que se transmite esa información dependerán muy estrechamente del medio de que se trate. La capa más baja de la pila de protocolos TCP/IP, la capa de acceso a la red, es la única que tiene que conocer cómo se transmite información a través del medio físico. Al resto de capas les es indiferente el medio a través del cual se va a transmitir la información.

Toda la lógica o mecanismos para codificar información que pueda ser transmitida está en la propia tarjeta de red. Existen distintas tarjetas de red: fibra óptica, cable coaxial, red inalámbrica, etc. Podemos clasificar los medios físicos en:

- **Medios guiados:** Pertenecen a este grupo todos aquellos medios de transmisión que tienen un soporte físico, es decir, cables de algún tipo. Los medios guiados más utilizados son:
    - **Cable coaxial:** El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central (conductor interno) rodeado por una malla y separados ambos elementos conductores por un cilindro de plástico. La velocidad máxima que se puede alcanzar es de 10Mbps. Hay de dos impedancias (resistencia):
        - Cable coaxial de banda ancha o de 75 ohmios. Es el que se utiliza en televisión por cable.
        - Cable coaxial de banda base o de 50 ohmios. Es el que se utiliza en las redes.
    - **Par trenzado:** Consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de 1 mm aproximado. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares). Existen varias modalidades de cables de par trenzado:
        - **Cable de par trenzado apantallado (STP)** En este tipo de cable, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. No se suele utilizar en las redes comunes porque es cable robusto, caro y difícil de instalar. El RJ49
        - **Cable de par trenzado con pantalla global (FTP).** En este tipo de cable, los pares no están apantallados, pero sí se dispone de una pantalla global

para mejorar su nivel de protección ante interferencias externas. El RJ45.

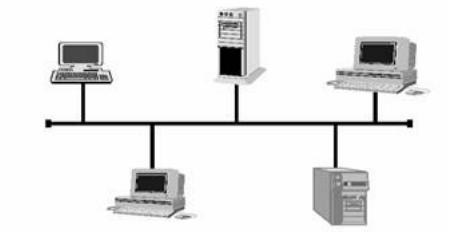
- **Cable de par trenzado no apantallado (UTP)**. Este es el cable de par trenzado más empleado por su simpleza, bajo costo, accesibilidad y fácil instalación. No tiene ningún tipo de pantalla adicional. El RJ45.
  - **Categoría 1**. Consta de dos pares de hilos. Para líneas de teléfonocon un máximo de velocidades de hasta 4 Mbps
  - **Categoría 3**. Consta de cuatro pares de hilos. Es utilizado en redes de datos. Alcanza velocidades de 10 Mbps.
  - **Categoría 5**. Consta de cuatro pares de hilos. Es el más utilizado en redes de datos en la actualidad. Alcanza velocidades de 100 Mbps.
  - **Categorías 6 y 7**. Consta de cuatro pares de hilos. Es el que se utilizará en las redes en un futuro cercano. Alcanza velocidades de 1 Gbps. Fullduplex

- **Fibra óptica**. La fibra óptica es un hilo fino generalmente de vidrio o plástico, cuyo grosor puede asemejarse al de un cabello, capaz de conducir la luz por su interior. En los cables de fibra óptica la información se transmite en forma de pulsos de luz (modulando su frecuencia) de tipo infrarrojo, no visible al ojo humano. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que puede emitir luz, y en el otro extremo se sitúa un detector de luz. Curiosamente, y a pesar de este sencillo funcionamiento, mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps y además, no se ven afectados por interferencias.

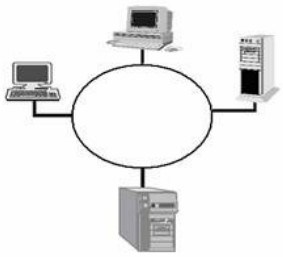
- **Medios no guiados:** Pertenecen a este grupo todos aquellos medios de transmisión que no tienen un soporte físico. Este tipo de medios suelen conocerse también con el nombre de **medios inalámbricos**. Los mas utilizados son:
  - **Ondas de radio**. Es el medio más utilizado en las pequeñas redes inalámbricas. Se propagan en todas las direccion y recorren grandes distancias. Su principal problema son las interferencias
  - **Infrarrojos**. Son ondas direccionales incapaces de atravesar objetos sólidos que están indicadas para transmisiones de corta distancia. Su principal inconveniente es que tiene que haber una línea de visión directa entre el emisor y el receptor del rayo infrarrojo.
  - **Microondas**. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Se utilizan para recorrer grandes distancias. Dos repetidores no deben exceder de unos 80 Kms. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas

Se entiende por **topología** de una red a la disposición en la que se encuentran dispuestos los ordenadores que la componen. Las más comunes son:

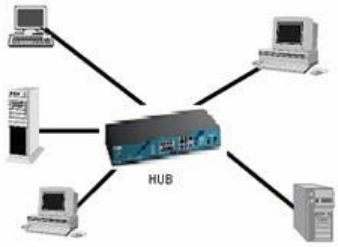
- **Topología en bus**. Esta topología viene caracterizada por la existencia de un cable lineal (un cable de tipo coaxial) al cual están conectados todos los equipos de la red. Cada equipo está conectado a dicho cable mediante un conector en T en cuyos extremos se añaden conectores BNC. Para evitar el rebote de la señal se coloca en los extremos de la red un elemento llamado **terminador**. Para empalmes de cable habrá que usar un elemento llamado empalmador BNC.



- **Topología en anillo**. Esta topología es un caso particular de la topología en bus en la que el cable de red está unido por los extremos, quedando el bus cerrado en forma de anillo. El cable es el coaxial, como en el bus, y se utilizan los mismos tipos de conectores, excepto los terminadores. Algunas redes de fibra óptica (FDDI) también presentan una topología en anillo.



- **Topología en estrella**. Esta topología es la más utilizada. En ella todos los equipos se encuentran conectados mediante un cable, generalmente de par trenzado, a un elemento central llamado concentrador o hub. Este elemento es el que hace de nexo de unión entre ellos y su misión es la de enviar la información recibida por una de sus conexiones al resto. Cuando se trata de una topología en estrella de par trenzado, cada equipo está conectado al hub/switch mediante un cable de par trenzado UTP-CAT5 (UTP Categoría 5) y conectores RJ45. Podría utilizarse como punto central un conmutador o switch.



Comunicación a través de un enlace o medio físico

Transmitir la información por un medio físico incluye básicamente dos aspectos.

- El primero de ellos, como ya hemos visto, era todo lo relativo a la definición y especificación de los **medios físicos** utilizables, así como a la disposición física de los equipos respecto a su conexión a dicho medio físico.

- Es ahora el momento de analizar el segundo de los aspectos que tienen que establecerse en este nivel, que es cómo se va a producir la **coordinación de la comunicación entre dos equipos o hosts a través de dicho medio físico**, también llamado enlace, para que ésta pueda llevarse a cabo con éxito.

Básicamente podemos encontrarnos con dos situaciones:

- Los dos equipos o hosts que quieren comunicarse se encuentran conectados a un **medio físico que es de uso exclusivo** suyo. Son los únicos conectados al medio físico. Se trata de una **comunicación por un enlace punto a punto**.
- Los dos equipos o hosts que quieren comunicarse se encuentran conectados a un **medio físico que es de uso compartido con otros equipos**. No son los únicos conectados al medio físico. Este tendrá que tener algún mecanismo que permita administrar y repartir el uso de dicho medio entre los distintos equipos que quieren hacer uso de él. Se trata de una **comunicación por un enlace compartido**, y al mecanismo para el reparto del uso del medio físico se le llama **algoritmo de arbitraje o de control de acceso al medio**.

Las tareas comunes son:

- **Control de errores**: Es imprescindible ser capaz de detectar estos errores en la transmisión así como ser capaz de subsanarlos y el protocolo del nivel de acceso a la red debe incorporar mecanismos que permitan realizar ambas tareas.

- **Control de flujo:** Cuando un equipo recibe información, ésta es almacenada en algún buffer, o espacio reservado de memoria hasta que puede ser procesada o tratada. Este buffer es limitado. Si el receptor se vería inundado (overflow) por la información, esta empezaría a perderse. Los algoritmos de control de flujo se encargan de organizar los flujos de información de tal manera que haya una cierta coordinación entre el receptor y el emisor

- **Multiplexión de varios enlaces lógicos:** El nivel de acceso a la red ofrece al nivel superior de la pila de protocolos un servicio: una comunicación fiable y sin errores con otro equipo que se encuentre también conectado al medio físico. Esto es lo que se llama multiplexar (superponer pero sin que se interfieran) varios enlaces lógicos (varias comunicaciones o conversaciones) sobre un mismo enlace físico (sobre un mismo medio).

- **Definición del formato de la trama:** la información no puede ser introducida de manera continua en el medio, sino que tiene que ser troceada en unidades de un tamaño máximo que son transmitidas individualmente. Se llama **trama** a cada una de estas unidades de información que son inyectadas en el medio físico. Estas tramas, aparte de la información en sí que se quiere transmitir, tienen que contener cierta información de control, como por ejemplo:
    - delimitadores de inicio y fin de trama,
    - direcciones de origen y destino de la trama,
    - información sobre la longitud de la trama,
    - información de flujo,
    - información para control de errores,
    - información útil para el arbitraje de acceso al medio, etc.

Comunicación por el enlace de un medio compartido

La mayoría de las redes de área local son **redes de difusión**; es decir, redes en las que existe un único canal de comunicación al que están conectados todos los equipos de la red y a través del cual tienen que transmitir todos ellos. En este tipo de redes el canal de comunicación es considerado como un recurso compartido de uso exclusivo por el que compiten todos los equipos conectados a la red y, por tanto, tendrá que haber un mecanismo que arbitre su uso. Dicho

mecanismo o protocolo recibe el nombre de **protocolo de control de acceso al medio** (MAC - Medium Access Control). Existen dos estrategias que son:

- **Paso del testigo.** Esta estrategia se basa en el establecimiento de un mecanismo de turnos para distribuir el uso del medio físico. Cada equipo tiene que esperar a que le llegue el turno para poder transmitir y tiene que encargarse de pasar el testigo o turno al siguiente equipo. Este tipo de estrategia es aplicable tanto en redes de difusión con topología en bus o estrella (norma 802.4, tambien conocida como token-bus) y en anillo (norma 802.5)
- **Contenida.** Esta estrategia no contempla turnos, sino una "lucha encarnizada" por la obtención del medio compartido. Cada equipo es libre de transmitir cuando así lo necesite y es a posteriori cuando se resuelven los conflictos. Este tipo de estrategia es aplicable sólo en topologías en bus (por consiguiente, también en estrella) y se sigue la norma 802.3, también conocida con el nombre CSMA-CD

Hay dos clases de tareas bien diferenciadas en la comunicación:

- las que se encargan de gestionar la correcta **comunicación** entre los dos equipos implicados en la comunicación (control de errores, control de flujo y multiplexación de varios enlaces lógicos) y
- las que se encargan de solucionar la problemática de encontrarse en un medio **compartido** cuyo uso hay que repartir entre todos los equipos conectados (control de acceso al medio).

Esto da lugar a una división en dos subniveles independientes:

- **Control Lógico del Enlace** (LLC - Logical Link Control). Se encarga de las tareas relacionadas con la gestión de una comunicación fiable, fluida y libre de errores.
- **Control de Acceso al Medio** (MAC - Medium Access Control). Se encarga de las tareas relacionadas con el arbitraje del medio compartido.

Direccionamiento MAC

En una red de difusión, el medio es compartido, lo que quiere decir que todos los equipos conectados "oyen" lo que pasa a través del mismo pero sólo el equipo al que va dirigida la información debe "escucharla". Independientemente del protocolo MAC concreto que se esté utilizando, existe un mecanismo de direccionamiento a este nivel para que los equipos sepan si la información que en un instante dado circula por el canal va dirigida a ellos o no. Es lo que se llama **dirección física o dirección MAC** de un equipo.

Más concretamente **esta dirección pertenece a la tarjeta de red**, pues la dirección va asociada a ella (un equipo con dos tarjetas de red tiene dos direcciones MAC, una por tarjeta) **y la llevan almacenada en una pequeña memoria que poseen las propias tarjetas.** Esta dirección les viene asignada de fábrica y no se puede variar. La dirección MAC de cada tarjeta de red es única en el mundo.

Una dirección MAC está formada por 48 bits, agrupados en seis octetos, donde cada octeto se representa por dos dígitos hexadecimales (xx:xx:xx:xx:xx:xx). Por ejemplo, 5D:1E:23:10:9F:A3. Existe una dirección MAC especial, la FF:FF:FF:FF:FF:FF (todos los bits a 1 en la dirección), que es lo que se llama **dirección broadcast o dirección de difusión**. Cuando una trama tiene como dirección de destino esta dirección, es escuchada y procesada por todos los equipos que se encuentran conectados al medio. Por tanto, la dirección broadcast representa a todos lo equipos de la red de área local.

Redes Ethernet

Ethernet es la solución comercial más extendida en una LAN que sigue la norma 802.3; es decir, que sigue una estrategia de acceso al medio de contienda en un medio compartido con topología en bus (de cable coaxial fino o grueso) o topología en estrella (de cable par trenzado o fibra óptica). Concretamente contempla los siguientes tipos de cableado (La nomenclatura que se usa para describir los tipos de cableado es la siguiente: Velocidad - Tipo de señal - Longitud/tipo de cable):

- **10Base5**. También conocida como **Ethernet gruesa**. Utiliza cable coaxial grueso de 50 ohmios de impedancia (banda base) y sigue una topología en bus. Se pueden llegar a alcanzar velocidades de hasta 10 Mbps. Puede alcanzar una longitud de hasta 500 metros, no pudiéndose conectar más de 100 equipos.
- **10Base2**. También conocida como **Ethernet fina**, más económica a la 10Base5; de hecho es mucho más utilizada. Utiliza cable coaxial fino de 50 ohmios de impedancia (banda base) y sigue una topología en bus. Se pueden llegar a alcanzar velocidades de hasta 10 Mbps. Puede alcanzar una longitud de hasta 185 metros (casi 200), no pudiéndose conectar más de 30 equipos.
- **10BaseT**. Esta modalidad de Ethernet es probablemente la más utilizada en la actualidad. Utiliza cable par trenzado no apantallado (UTP con conectores RJ45) de 100 metros de longitud máxima, con una topología en estrella (uso de un hub). Se pueden llegar a alcanzar velocidades de hasta 10 Mbps.
- **10BaseFL**. Esta modalidad de Ethernet utiliza fibra óptica con una topología en estrella y con una velocidad máxima de hasta 10 Mbps. Con el uso de fibra óptica se puede cubrir mayores distancias en la red de área local (varios kilómetros)
- **100BaseT** y **100BaseFL**. También conocidas como Fast-Ethernet, funcionan a velocidades de 100 Mbps con cable de par trenzado y fibra óptica respectivamente.

Veamos ahora cómo funciona el protocolo de contienda de control de acceso al medio CSMA/CD (norma 802.3) utilizado en las redes Ethernet. El término CSMA/CD significa "Carrier Sense, Multiple Access with Collision Detection"; es decir, "Acceso multiple por detección de portadora con detección de colisiones". Analicemos detenidamente qué significa esto.

Es probable que dos equipos coincidan en la transmisión de datos por el medio, bien porque transmiten al mismo tiempo o bien porque uno empiece a transmitir cuando el otro todavía no ha acabado de hacerlo. Esta circunstancia recibe el nombre de **colisión** y cuando se produce, los datos que circulan por el medio quedan dañados e inservibles, viéndose los equipos involucrados obligados a retransmitir los datos nuevamente. Es de vital importancia reducir al mínimo el número de colisiones.

- Cuando un equipo necesita transmitir datos, primero escucha el medio para comprobar si hay algún otro equipo transmitiendo,
- si el medio está inactivo inicia la transmisión, mientras que,
- si el medio está ocupado se espera unos microsegundos antes de volverlo a intentar.

A esta acción de comprobar la actividad del medio antes de emitir se la conoce con el nombre de "**detección de portadora**".

Otra de las características de este protocolo es que, un equipo, al mismo tiempo que está emitiendo, está comprobando si se produce una colisión. Si se detecta una la colisión el equipo interrumpe su transmisión y no termina de transmitir su trama (pues una vez que se produce una colisión la información queda mutilada y es ya irrecuperable). Esto se traduce en un ahorro de tiempo y en un mejor aprovechamiento de la red. Este mecanismo de interrupción inmediata de la transmisión nada más detectarse una colisión se conoce con el nombre de "**detección de colisión**".

Otros elementos presentes en las LAN

Si queremos conectar dos redes que están más lejos de lo permitido, tenemos dos opciones: montar otra red de área local totalmente distinta a la existente o hacer uso de unos elementos que sirvan de "empalme" entre la LAN ya existente y el nuevo segmento que se añada.

Estos elementos que pueden hacer de enlace o "empalme" entre dos segmentos distintos de una misma LAN, son los siguientes:

- **Hub o concentrador**. Es lo que se llama un dispositivo "tonto", pues lo único que hace es reenviar lo que recibe por una de sus entradas al resto de ellas, simulando la existencia de un medio compartido. En cada puerto (entrada) del dispositivo puede haber conectado un equipo individual o un segmento completo de la LAN.
- **Switch o conmutador**. Es un dispositivo que cuenta con cierta "inteligencia", pues:
    - capaz de escuchar y aprender las direcciones MAC
    - lo hace dinámicamente escuchando las tramas que circulan por la LAN y asociando la dirección de origen de la trama con el puerto por el que le llega dicha trama.
    - De esta manera, en vez de reenviar una trama por todos los puertos para simular un medio compartido, sólo tendrá que mandarlo por aquella entrada en la que ha aprendido que se encuentra el equipo destino de la trama.
    - En cada puerto (entrada) del dispositivo puede haber conectado un equipo individual o un segmento completo de la LAN. En este último caso, para esa entrada aprenderá más de una dirección MAC, la de todos los equipos del segmento.
    - el uso de un switch reducirá considerablemente el tráfico y aumentará la eficiencia de la LAN.
- **Bridge o puente**. Este elemento tiene la misma "inteligencia" que un switch y la única diferencia con respecto a éste es que, además, es capaz de hacer de enlace o "empalme" entre dos redes que siguen normas distintas de funcionamiento;

Comunicación por el enlace punto a punto

Un enlace punto a punto entre dos equipos es un medio físico compartido única y exclusivamente por esos dos equipos a través del cual se pueden comunicar. En estos casos no es necesario ningún mecanismo de arbitraje para acceder al medio, pues éste tan sólo es compartido por esos dos equipos. Por otra parte, sí será necesario llevar a cabo el resto de tareas asociadas a este nivel de la pila de protocolos: control de flujo, control de errores y multiplexación de varios enlaces lógicos sobre un mismo enlace físico. Un ejemplo es internet, el equipo del usuario tiene que conectarse a un equipo de su proveedor de Internet, que es el que le dará acceso o salida a la red.

Los dos protocolos más utilizados para comunicaciones punto a punto son:

- **SLIP** (Serial Line Internet Protocol - Protocolo para redes punto a punto) y
- **PPP** (Point to Point Protocol - Protocolo Punto a Punto). Es apto para su uso en líneas telefónicas conmutadas y, además, permite al proveedor de servicio asignar dinámicamente las direcciones IP a sus clientes, algo muy común actualmente. Permite

configurar el tamaño máximo de la trama que puede circular por el enlace MTU)

6. Redes (II)

Fundamentos generales de nivel de interred

El nivel de interred o nivel de red de la pila de protocolos TCP/IP es el que dará solución a toda esta problemática para hacer posible la comunicación cuando nos encontramos en un escenario donde hay interconectadas una serie de redes heterogéneas. La principal misión del nivel de red es la de abstraer a los niveles superiores de la localización física de los equipos que participan en la comunicación. Es decir, este nivel se compromete a hacer llegar la información desde el equipo origen al equipo destino, independientemente del número y tipología de las redes que haya que atravesar a lo largo del trayecto entre estos dos puntos. El nivel de red presenta a los niveles superiores una visión homogénea de todas las redes (habitualmente heterogéneas) interconectadas que forman la interred. Los niveles superiores de la pila de protocolos tan sólo tienen que decirle al nivel de red con qué equipo quiere establecer una comunicación y entregarle a dicho nivel la información a transmitir, despreocupándose de toda la problemática derivada del encaminamiento de la información del equipo origen al equipo destino. Presenta a los niveles superiores una visión homogénea de todas las redes heterogéneas interconectadas que forman la interred.

Los Routers o Encaminadores

Imaginamos una ciudad nueva, y tienes que ir a un destino. En cada cruce de calle hay un guardia que te indica por donde tienes que ir. Cada calle del ejemplo sería una red, mientras que los guardias de tráfico reciben aquí el nombre de encaminadores o routers.

Los routers o encaminadores son equipos conectados a varias redes y que tienen capacidad para encaminar la información que reciben hacia el destino al que ésta va dirigida. Estas decisiones de encaminamiento se toman en base a una serie de **algoritmos de encaminamiento** o de ruteo, que son los que gestionan este tipo de información. Un buen algoritmo de encaminamiento es aquél en el que se consiguen los siguientes objetivos:

- **Ser capaz de adaptarse dinámicamente a los cambios que se produzcan en el mapa de interconexión.** La realidad de las redes de ordenadores es una realidad dinámica.

- **Ser capaz de encaminar o enviar la información por el camino por el que se tarde menos tiempo en alcanzar el destino**. Intervienen dos factores:
    - el número de routers intermedios o redes que hay que atravesar y
    - la congestión o tráfico existente en dichas redes intermedias en ese instante dado.

Intercambio de información en la red

Los routers o encaminadores deben intercambiar información para comunicar al resto de routers el estado de las redes que ellos interconectan y así, al contar con una imagen global del estado de la interred, poder tomar mejores decisiones de encaminamiento.

Protocolos de nivel de red que intervienen en los equipos terminales o hosts. Entre dichos protocolos destacamos:

- **El protocolo IP o Internet Protocol (Protocolo de Interred)**. Éste es el protocolo principal del nivel de red en la pila de protocolos TCP/IP. Se encarga de definir tanto el

direccionamiento a nivel de red como el formato de la información de control asociada a dicho nivel. Actualmente se utiliza una versión de este protocolo conocida con el nombre de IP versión 4 o IPv4. En un futuro no muy lejano será sustituida por Ipv6

- **El protocolo ARP o Address Resolution Protocol (Protocolo para la resolución de direcciones)**. Es un protocolo secundario, también del nivel de red, que sirve para hacer traducciones entre direcciones de nivel de red (direcciones IP) y direcciones de nivel de acceso a la red (direcciones MAC). Este protocolo está asociado a IPv4; en IPv6 no se utiliza.

- **El protocolo ICMP o Internet Control Message Protocol (Protocolo de mensajes de control en la Interred)**. Este es un protocolo de control de ciertos errores a nivel de red. La versión ICMPv4 se utiliza con IPv4, la versión ICMPv6 se utiliza con IPv6.

Introducción al protocolo IPv4

Su misión principal es la de definir tanto el direccionamiento a nivel de red como el formato de la información de control asociada a dicho nivel. Como sabemos, cada nivel de la pila de protocolos recibe los datos del nivel superior que, junto a la información de control del nivel correspondiente, forman la unidad de datos de éste. La unidad de datos del nivel de red IP se llama **paquete o paquete IP**. Por lo tanto, un paquete IP está formado por los datos del nivel de transporte, más información de control del propio nivel de red. Por otra parte IP es un protocolo que ofrece al nivel superior o nivel de transporte un servicio con las siguientes características:

- **No garantiza que los paquetes lleguen a su destino en el mismo orden en el que son enviados.** Cada paquete es enrutado de forma independiente y debe contener la IP de destino. Cada uno puede coger por diferentes caminos por lo que es imposible gatirantizar que llegarán

- **No se garantiza que los paquetes lleguen a su destino sin errores en los datos**. Sólo detecta los errores que se producen en los propios datos de control del nivel de red, pero no los que se producen en el nivel superior

- **Ni siquiera se garantiza la entrega de los paquetes que se envían**. En casos de gran congestión en la red los routers pueden verse desbordados (más paquetes de lo que puede almacenar en el buffer). Los routers tienen permiso para eliminar los paquetes de más que les llegan y se perderán

Será la capa de nivel superior, la capa de transporte, la que trate toda esta problemática

Direccionamiento unicast de IPv4

Para poder llegar a un ordenador dentro de una interred, éste deberá tener una dirección que lo identifique de manera única y que nos permita saber cómo localizarlo. Cada equipo conectado a una interred tiene que tener una dirección que lo identifique unívocamente. Esta dirección recibe el nombre de dirección IP y realmente, no se asocia a un equipo, sino a una interfaz de red o tarjeta de red del equipo. Toda dirección IPv4 tiene 32 bits (4 bytes u octetos) y debe ser única; es decir, no puede haber dos equipos que tengan asignada la misma dirección IP.

Este tipo de direcciones que sirven para identificar a un equipo concreto dentro de la interred reciben el nombre de **direcciones unicast**. Una dirección unicast se divide conceptualmente en dos campos:

- **Campo identificador de red (netid).** Identifica a la red a la que está conectado el host.
- **Campo identificador de host (hostid).** Identifica al host dentro de la red específica.

Objetivos del direccionamiento UNICAST

- **Disminuir** la cantidad de información que los routers deben manejar para tomar las decisiones de encaminamiento.
- **Agilizar** los algoritmos de encaminamiento
- **Garantizar** que equipos de una misma organización tengan direcciones IP consecutivas

Clases de Redes

Observamos que:

- el tamaño o número de bits que se establezca para el identificador de red influirá en el número de redes posibles en una interred,
- mientras que el tamaño o número de bits que se establezca para el identificador de host influirá en el número de equipos que pueden estar conectados a una misma red.

¿qué tamaño es el adecuado fijar para cada uno de estos campos? Se adoptan tres tipos o clases (para establecer la clase a la que pertenece una dirección se utilizan los primeros bits de la misma):

- **Direcciones de Clase A**. 7 bits para el identificador de red y 24 bits para el identificador de host. 2^7 = 128 redes y 2^{24} = 16 777 216 equipos. Comienzan por 0 (el primer bit de la dirección).
- **Direcciones de Clase B**. 14 bits para el identificador de red y 16 bits para el identificador de host. 2^{14} = 16 384 redes y 2^{16} = 65 536 equipos. Comienzan por 10 (los 2 primeros bits de la dirección).
- **Direcciones de Clase C**. 21 bits para el identificador de red y 8 bits para el identificador de host. 2^{21} = 2 097 152 redes y 2^8 = 256 equipos. Comienzan por 110 (los 3 primeros bits de la dirección).

Conocer la clase a la que pertenece una dirección IPv4 es fundamental para interpretar los bits que la componen de una manera o de otra.

Notacion decimal para las direcciones IPv4

Para que las direcciones IP sean un poco más manejables por las personas, ya que es imposible que lleguemos a memorizar los 32 bits de cada dirección, se ideó una representación especial de direcciones IP, llamada **notación decimal o notación punto**. En esta notación cada uno de los cuatro octetos de la dirección IP se sustituye por su número decimal correspondiente, que estará entre 0 y 255 (8 bits)

Observando la dirección 192.168.5.205, sabemos que es de tipo C, pues empieza por los bits 110. Por lo tanto, el identificador de red viene dado por los tres primeros octetos (192.168.5), mientras que el identificador de host viene dado por el último octeto (205). Esto quiere decir que la dirección anterior identifica al host 205 dentro de la red IP 192.168.5.

Direcciones especiales en IPv4

Existen ciertas combinaciones de bits, es decir, ciertas direcciones IP, que tienen un uso y significado especial y que no pueden utilizarse como el resto. Son:

- No se puede asignar a ningún equipo una dirección IP en la que el **identificador de host tenga un valor de todo a cero**. Este tipo de dirección se utiliza para identificar a una red en sí y es por eso que no puede ser asignada a ningún host de dicha red. Estas direcciones son las que utilizan, por ejemplo, los routers para identificar a una red en las tablas de enrutamiento que utilizan sus algoritmos de enrutamiento. Ej: 5.0.0.0

- No se puede asignar a ningún equipo una dirección IP en la que el **identificador de host tenga un valor de todo a uno**. Este tipo de dirección representa a todos los equipos de la red indicada en el identificador de red correspondiente. Esto es lo que se llama **broadcast o difusión dirigida a nivel IP**. Ej: 5.255.255.255

- La red que viene dada por el **identificador de red cuyo valor sea de todo a cero**, no existe. Este tipo de identificador se interpreta como "esta red". Ej: 0.125.3.34. La utilización de este tipo de direcciones tan sólo está permitida durante el procedimiento de arranque del sistema y sirve para permitir que una máquina se comunique temporalmente mientras aprende cuál es su dirección de red y dirección IP correctas.

- La dirección en la que tanto el **identificador de red como el identificador de host tiene un valor de todo a cero**, la puede utilizar un equipo para referirse a sí mismo. La utilización de este tipo de dirección tan sólo está permitida durante el procedimiento de arranque del sistema mientras se aprende la dirección de la red a la que pertenece y su dirección IP correcta.

- La dirección en la que tanto el **identificador de red como el identificador de host tiene un valor de todo a uno** hace referencia a todos los equipos de la interred. Evidentemente, esto no se permite para evitar el caos en esta red global; los routers no dejan pasar este tipo de tráfico. Esta dirección **equivale a un broadcast en la propia red a la que se está conectado**. Se suele utilizar en el arranque y mandar un mensaje a todos los equipos de la misma.

- **La subred de clase A 127.0.0.0** no puede ser asignada a ninguna red. Todas las direcciones de esta red se utilizan para realizar comprobaciones de que la pila TCP/IP está operativa dentro del propio equipo. En la práctica sólo se usa la **dirección 127.0.0.1**, también conocida como **dirección de loopback.** Los mensajes enviados a esta dirección nunca abandonan el host local; es decir, no producen tráfico en la red.

Con estas restricciones afirmamos:

- cada red de clase A puede albergar 2^{24} - 2 = 16 777 214 equipos.
- cada red de clase B puede albergar 2^{16} - 2 = 65 534 equipos.
- cada red de clase C puede albergar 2^{8} - 2 = 254 equipos.

Concepto de subred IP

En principio, y por definición, todos los equipos que pertenecen a una misma red IP deben poder comunicarse directamente a través del medio. Por el contrario, equipos que no pertenecen a una misma red IP deberán utilizar elementos intermedios, los routers, para poder comunicarse. Si reflexionamos sobre la afirmación anterior, observamos que esto puede suponer un problema,

sobre todo para organizaciones que poseen redes de tipo A o B. Estas redes están ideadas para alojar multitud de equipos; sin embargo, como sabemos, en un mismo medio físico resulta imposible conectar un número tan elevado de ellos. Para solucionar el problema se ideó el concepto de **subred IP**.

Las subredes son redes físicamente independientes que comparten una misma dirección IP. Ésta ahora se interpreta de una manera un poco distinta, para dar cabida al concepto de subred. De los 32 bits que conforman la dirección IP:

- Los bits pertenecientes a la parte de identificador de red se siguen interpretando exactamente igual.
- Los bits pertenecientes a la parte de identificador de host se dividen en dos bloques: una parte servirá para identificar a la subred y otra parte servirá para identificar al host dentro de dicha subred.

Todos los equipos que pertenezcan a una misma subred IP deben poder comunicarse directamente a través del medio (el cual comparten), mientras que aquéllos que no pertenezcan a la misma subred IP tendrán que utilizar algún elemento intermedio, un router, para poder establecer una comunicación.

Proceso de comunicación en una interred

Vamos a ver cómo el nivel de red cumple con su objetivo, que es el de **hacer llegar la información desde el equipo origen al equipo destino, se encuentren éstos donde se encuentren dentro de la interred**.

Cuando en el nivel de red, un equipo quiere establecer una comunicación con otro del cual conoce su dirección IP, tiene que realizar los siguientes pasos:

- Tiene que averiguar si comparte el medio físico con dicho equipo; es decir si dicho equipo se encuentra en la misma subred IP que él, o en la misma red en el caso de que se encontrase en una red IP no dividida en subredes.
- De ser así, entonces sabe que puede mandarle directamente la información a través del medio que comparten.
- En caso contrario, tendrá que mandarle la información al router por defecto de su subred, que es el que sabrá cómo encaminar dicha información para que llegue a su destino

Algoritmo para evaluar si dos equipo comparten el medio físico

Dada una dirección IP de destino,¿cómo sabe un equipo si comparte el medio físico con el host al que pertenece dicha IP? **Sin la existencia del concepto de subred** no habría ningún problema para interpretar una dirección IP según la clase de dirección a la que pertenezca. Si la parte de identificador de red del equipo destino coincidiese con la parte de identificador de red del equipo origen, éste sabría que ambos se encuentran en la misma red IP y, consecuentemente, compartirían el mismo medio.

Con la aparición del concepto de subred, cada organización es libre para dividir en subredes la red IP que tiene asignada, y eso obliga a que exista algún mecanismo para controlar el problema. Para ello se utiliza lo que se conoce con el nombre de **máscara de red**, dicho más correctamente, **máscara de subred**. Ésta no es más que una secuencia de 32 bits en la que están puestas a uno aquellas posiciones de la dirección IP que se corresponden con el campo identificador de red y de subred de la misma y están puestas a cero aquellas posiciones de la dirección IP que se corresponden con el campo identificador de host.

Consideraciones sobre la máscara de subred

- Las máscaras de red asociadas a las redes en las que no hay subdivisión en subredes, es decir, aquéllas en las que se sigue el formato de dirección puro definido por la clase de la dirección, son las siguientes:
    - 255.0.0.0 para las de clase A,
    - 255.255.0.0 para las de clase B y
    - 255.255.255.0 para las de clase C.

  si un ordenador cuya dirección IP es de una clase y su máscara contiene más unos de los establecidos para la máscara estándar de esa clase, entonces es porque dicho ordenador se encuentra en una red dividida en subredes

- Cuando una red está subdividida en subredes, todos los equipos de dicha red deben tener el mismo esquema de subred; es decir, la misma máscara.

- Es necesario configurar la máscara de subred utilizando unos en los bits que corresponden al campo identificador de red de la clase de dirección. Por ejemplo, una máscara de subred 255.255.0.0 no es válida en una dirección de clase C, pues al menos los bits del identificador de red deben estar a uno; es decir, 255.255.255.0.

- Todo equipo de una red conoce tanto su propia dirección IP como su máscara de red, la cual le dice cómo debe interpretar el campo identificador de host de su dirección.

Cuando un equipo quiere comunicarse con otro, del cual sólo conoce su dirección IP, para saber si comparte el medio físico con él, siempre lleva a cabo el siguiente procedimiento, independientemente de que se encuentre en un entorno con subredes o no:

- Realiza un AND lógico entre su dirección IP y su máscara de red. De esta manera, obtendrá la red o subred, en su caso, a la que pertenece.

- Igualmente, hace un AND lógico entre su propia máscara y la dirección IP del equipo destino con el que se quiere comunicar.

- Si el resultado de ambas operaciones es el mismo, entonces es porque ambos equipos pertenecen a la misma red IP, o subred en su caso, y por tanto, comparten el mismo medio físico a través del cual se podrán comunicar directamente.

Comunicación cuando fuente y destino comparten el mismo medio

Si el equipo destino con el que el equipo fuente quiere establecer una comunicación se encuentra en su misma subred, esta comunicación puede realizarse directamente a través del medio que comparten, de la siguiente manera:

- El nivel de red del equipo fuente encapsulará la información que recibe del nivel superior en un paquete IPv4 que irá dirigido a la dirección IP del equipo destino.
- Asimismo, el nivel de acceso a la red del equipo fuente encapsulará dicho paquete IP en una trama dirigida a la dirección MAC del equipo destino.
- Por su parte, el equipo destino recogerá la trama que va dirigida a él y desencapsulará el paquete IP contenido en su interior.
- Entonces comprobará que el paquete va dirigido a su dirección IP, desencapsulará la información contenida en el paquete y se la pasará a la capa superior.

Comunicación cuando fuente y destino no comparten el mismo medio

Si el equipo destino y el equipo fuente no se encuentran en su misma subred la comunicación se hace mediante **routers** o **encaminadores**, también llamados **Gateways o puertas de enlaces** en ciertos entornos. Los encaminadores IP o routers son, básicamente, hosts TCP/IP conectados a dos o más subredes para hacer de puente entre ellas.

El equipo fuente le entrega el paquete IP a uno de los routers de su subred. Posteriormente, dicho paquete irá pasando de router en router hasta que llegue a uno que pueda transmitir directamente el paquete al equipo destinatario del mismo, porque comparta subred con él. Generalmente sólo suele haber un router en cada subred y los equipos de la misma saben que, en caso de que tengan que comunicarse con un equipo externo, tienen que hacerlo a través de dicho router; es decir, lo tienen configurado como **router o gateway por defecto**. En caso de haber más de un router en la subred, los equipos deben tener información sobre a qué redes da acceso cada uno de ellos, aunque siempre existe especificado un router por defecto.

El procedimiento que se lleva a cabo en una comunicación cuando los equipos implicados no pertenecen a la misma subred IP es el siguiente:

- El nivel de red del equipo fuente encapsulará la información que recibe del nivel superior en un paquete IPv4 que irá dirigido a la dirección IP del equipo destino.
- Además, el nivel de acceso a la red del equipo fuente encapsulará dicho paquete IP en una trama dirigida a la dirección MAC del router correspondiente de su propia subred.
- Una vez que el router de la subred local recibe la trama que va dirigida a él, desencapsula el paquete IP que ésta contiene y analiza la dirección destino del mismo.
- Entonces, sus algoritmos de encaminamiento le dirán, en base a dicha dirección, cuál es el siguiente router al que tiene que mandar el paquete para que éste llegue a la red destino; es decir, le dirán cuál es el siguiente salto (next-hop) en el camino hacia el destino. Evidentemente, entre ambos routers tiene que existir siempre un medio compartido, por lo que la comunicación entre ellos es directa.
- Por lo tanto, el router encapsulará el paquete IP en una trama del nivel de acceso a la red correspondiente, la cual irá dirigida a la dirección MAC de este router que supone el siguiente salto en el camino.
- Este proceso se repite hasta que el paquete llega a un router que está conectado a la misma red a la que pertenece el equipo destino.
- Entonces este router encapsulará el paquete IP en una trama dirigida a la dirección MAC del destino, el cual la recogerá, desencapsulará el paquete IP contenido en su interior, comprobará que el paquete va dirigido a su dirección IP, desencapsulará la información contenida en el paquete y se la pasará a la capa superior de su pila de protocolos.

Protocolo ARP

Una vez que un equipo sabe a qué equipo de su subred debe entregarle el paquete IP, ya sea ésta la máquina destino real o ya sea al router de salida de la subred, ¿cómo sabe un equipo a qué dirección MAC debe enviar la trama?

Aquí es precisamente donde entra en acción el **protocolo ARP** (Address Resolution Protocol - Protocolo para la resolución de direcciones), cuya misión es la de proporcionar los mecanismos necesarios para poder averiguar la dirección MAC que se encuentra asociada a la dirección IP de un equipo que se encuentre compartiendo el medio físico (que pertenezca a la misma subred).

Para lograrlo se hace lo siguiente:

- Se emite un paquete especial llamado ARP Query (ARP de pregunta) dentro de una trama dirigida a todos los equipos que están conectados al medio; es decir, una trama broadcast, dirigida a la dirección MAC FF:FF:FF:FF:FF:FF. Dicho paquete ARP contiene:
    - Dirección MAC del equipo que está preguntando.
    - Dirección IP del equipo que está preguntando.
    - Dirección IP del equipo del que se quiere averiguar la dirección MAC.

- La trama la reciben todos los equipos. Cada equipo desencapsula el paquete ARP y lo pasa al nivel de red reconoce que se trata de un paquete ARP y procede a analizarlo. Cada equipo lee el campo de IP de destino y la compara con la suya, sólo uno reconocerá su dirección IP
- El equipo al que iba dirigido realmente el paquete ARP (y que ha reconocido su IP en el ARP Query) responderá con un paquete especial llamado **ARP Response** (**ARP de respuesta**) en el que le comunica al equipo que realizó la pregunta cuál es su dirección MAC. Será encapsulado en una trama dirigida a la dirección MAC del equipo que realizó la pregunta, con lo que le llegará únicamente a él. Contiene:
    - Dirección MAC del equipo que se buscaba, que es el que está generando este paquete de respuesta.
    - Dirección IP del equipo que se buscaba, que es el que está generando este paquete de respuesta.
    - Dirección MAC del equipo que realizó la pregunta y al cuál se está contestando con este paquete ARP.
    - Dirección IP del equipo que realizó la pregunta y al cuál se está contestando con este paquete ARP.
- Cuando el equipo que realizó la pregunta inicial recibe este paquete ARP de respuesta, analiza la información y averigua cuál es la dirección MAC asociada al equipo al que tiene que mandar el paquete IP. Entonces encapsula dicho paquete IP en una trama que vaya dirigida a esa dirección MAC y se la manda por el medio físico.

Los equipos van almacenando en una caché los pares (dirección IP, dirección MAC) que van aprendiendo y los mantienen durante un tiempo. Además, un equipo no aprende sólo aquellas direcciones por las que él mismo pregunta, sino todas las direcciones de cualquier equipo que pregunta. En el supuesto en el que un equipo quiera establecer una comunicación con un equipo que no pertenece a su subred, lo que tiene que hacer es enviarle el paquete IP al router de su subred que le dé salida al exterior. Evidentemente, la IP de dicho router la debe conocer. Entonces, utilizará el protocolo ARP para averiguar la dirección MAC del router.

No es posible averiguar la dirección MAC asociada a una IP externa a la subred, aparte de que no tiene sentido hacerlo.

Protocolo ICMPv4

Como el protocolo IP no ofrece ningún mecanismo para que el emisor pueda detectar si los paquetes que se están enviando están llegando bien, se ha ideado un mecanismo que permita a los routers ofrecerles cierto tipo de información sobre errores o situaciones no esperadas que puedan producirse en la red. Dicho mecanismo viene descrito por el protocolo **ICMP** (Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet). Permite:

- Informar de que el destino es inalcanzable.
- Informar de que un paquete ha sido eliminado de la red por exceso de tiempo.
- Informar a un emisor de paquetes de que la red está congestionada (hay mucho tráfico).

Sin embargo, su utilidad más extendida entre los usuarios de informática es la posibilidad que ofrece para averiguar si hay algún equipo que responda a una dirección IP concreta. Esto es lo que se conoce con el nombre de **ping** (mensaje ICMP especial dirigido a una dirección IP y conteniendo unos datos, que provoca que el equipo destino responda con otro mensaje ICMP que contiene los mismos datos).

Los mensajes ICMP viajan dentro de paquetes IP como si fuera un protocolo de nivel superior. Esto se hace para aprovechar la capacidad que tiene IP de hacer llegar información desde un origen a un destino a través de la interred. Por lo tanto no garantiza que llegará a destino. La existencia del protocolo ICMP no debe llevarnos a la confusión:

- El protocolo ICMP no soluciona el problema de la pérdida de paquetes ni evita que los paquetes no lleguen a su destino. Simplemente es un protocolo para que se pueda avisar al equipo emisor de ciertas situaciones de error en la red. Además el protocolo tampoco garantiza que ante una situación de error el emisor vaya a ser avisado.

- ICMP es un protocolo para informar de errores, no para corregirlos ni subsanarlos.

- IP sigue ofreciendo un servicio que no garantiza nada: ni asegura la entrega de paquetes sin errores, ni asegura que éstos sean entregados en el mismo orden en el que fueron enviados, ni siquiera asegura la entrega en sí de los paquetes. De hecho, cuando vía ICMP se le informa de una condición de error, IP simplemente se limita a avisar del error a los niveles superiores para que actúen en consecuencia.

Fundamentos del nivel de transporte

El nivel de red es el encargado de hacer llegar la información desde el origen al destino a través de la interred. Pero una vez que el nivel de red entrega la información en el equipo de destino es necesario saber a qué proceso o aplicación concreta dentro del equipo va destinada dicha información. El nivel de transporte se centra en tratar los aspectos necesarios para que aplicaciones que se encuentran en hosts distintos de la red puedan entablar una comunicación. Su objetivo es ocultar a dichas aplicaciones, que están por encima de él, la realidad de la red que tienen por debajo. Dichas aplicaciones ven la red como un servicio que les proporciona el nivel de transporte y que les permite mandarle información a aplicaciones remotas. Ellas sólo tienen que preocuparse de entregar los datos al nivel de transporte y éste ya se encargará de hacerlos llegar a la aplicación correspondiente en el equipo remoto.

El nivel de transporte es el primero de la pila de protocolos TCP/IP que funciona exclusivamente en ambos extremos de la comunicación; es decir, solamente en los hosts remotos que entablan una comunicación. Los routers, en sus tareas de encaminamiento, no conocen protocolo de transporte alguno, pues lo único que necesitan para hacer llegar los paquetes a su destino es la información de la cabecera IP. El mecanismo que utiliza el nivel de transporte de la pila de protocolos TCP/IP para identificar a la aplicación o proceso dentro del equipo remoto al que tiene que entregarse la información, es el mecanismo de **puertos**.

Desde el punto de vista del sistema operativo un puerto representa a un proceso, aplicación o tarea perteneciente al nivel de aplicación. Una aplicación se asocia a un puerto de tal manera que todo lo que llegue al equipo que vaya dirigido a ese puerto, será entregado por el nivel de transporte a esa aplicación. Se suele decir que la aplicación se encuentra "**escuchando ese**

puerto". Podemos considerar un puerto como una interfaz entre un programa concreto y la capa de transporte.

Existen un conjunto de puertos, denominados **puertos bien conocidos**, en los que la comunidad internacional ha fijado qué tipos de aplicaciones son las que van a estar escuchando. **Los puertos bien conocidos son los 1024 primeros (del 0 al 1023).**

- FTP (File Transfer Protocol) 20 y 21
- SSH (Secure Shell) 22
- Telnet 23
- SMTP (Simple Mail Transfer Protocol) 25
- servidor BOOTP (Servidor DHCP) 67
- cliente BOOTP (Cliente DHCP) 68
- HTTP (HyperText Transfer Protocol) 80
- POP3 (Post Office Protocol versión 3) 110

El nivel de transporte ofrece al nivel superior (nivel de aplicación) dos tipos distintos de servicios:

- Uno ofrecido a través del protocolo **TCP** (Transmisión Control Protocol - Protocolo de Control de Transmisión) que garantiza que:
    - Los datos llegarán a la aplicación destino en el mismo orden en que la aplicación origen los mande.
    - Los datos llegarán sin errores desde la aplicación origen a la aplicación destino
    - Los datos llegarán a su destino

  El protocolo TCP es el más importante de los protocolos de transporte, pues ofrece a las aplicaciones un servicio fiable, que es lo que se necesita en la mayoría de los casos. De hecho, es uno de los protocolos que da nombre a la pila TCP/IP.

- Otro ofrecido a través del protocolo **UDP** (User Datagram Protocol - Protocolo de Datagrama de Usuario) es un protocolo de transporte que:
    - No garantiza que los datos vayan a llegar a la aplicación destino en el mismo orden que la aplicación origen los mandó.
    - No garantiza que los datos lleguen sin errores desde la aplicación origen a la aplicación destino
    - Ni siquiera garantiza que los datos llegarán a su destino.

  De lo único que se encarga es de identificar a las aplicaciones implicadas en la comunicación, mediante el mecanismo de puertos y de ir transfiriéndoles la información destinada a ellas. Deberá ser la propia aplicación la que tenga que establecer sus propios mecanismos si quiere obtener algún tipo de garantía. Cuando usarlo:
    - comunicación entre las aplicaciones se realiza a través de mensajes que no necesitan confirmación de que han sido recibidos
    - comunicación entre las aplicaciones se realiza de forma esporádica.
    - La fiabilidad se implementa al nivel de la aplicación.
    - Hay incluso aplicaciones en las que un servicio TCP no les permitiría funcionar correctamente. El ejemplo más claro lo tenemos en las aplicaciones multimedia en tiempo real (videoconferencia, radio en tiempo real, telefonía IP, etc). Si este tipo de aplicaciones utilizasen el protocolo TCP, las pérdidas, errores y retransmisiones correspondientes ralentizarían la comunicación, haciendo imposible la sensación de "tiempo real".

En el mundo TCP/IP, una conexión entre dos equipos viene definida por los pares:

- *Dirección IP del equipo origen + número del puerto origen*
- Dirección IP del equipo destino + número del puerto destino

Fundamentos del nivel de aplicación

El verdadero trabajo que da utilidad a la red en sí, se lleva a cabo en la capa de aplicación. En esta capa es donde se definen los protocolos que establecen, entre otras cosas, las reglas a seguir durante la comunicación entre dos aplicaciones remotas, los mecanismos y actuaciones empleados y el formato de la información que se va a intercambiar durante dicha comunicación. Evidentemente, en esta capa tienen cabida infinidad de protocolos, cada uno de los cuales describe la comunicación entre dos aplicaciones de red.

Existen una serie de protocolos ya establecidos que definen cómo debe procederse para llevar a cabo los servicios básicos de red como son:

- el servicio de correo,
- el servicio de transferencia de archivos,
- el servicio de terminal remoto, etc.

Esto no quiere decir que no puedan idearse otros protocolos para proporcionar los mismos servicios. Simplemente quiere decir que estos protocolos han sido mundialmente aceptados por la comunidad Internet y son los que se usan actualmente para proporcionar estos servicios. Podemos agrupar los protocolos existentes en el nivel de aplicación en las siguientes dos categorías:

- Protocolos de infraestructura TCP/IP, que son protocolos que facilitan el uso de la red.

- Protocolos de aplicación, que son protocolos que utilizarán los usuarios con un propósito de comunicación, como por ejemplo, transferir ficheros entre dos ordenadores, mantener una conversación mediante chat, etc.

De entre los protocolos de infraestructura TCP/IP destacamos los siguientes:

- Protocolo DHCP, que es un protocolo para que los hosts puedan configurar automáticamente sus parámetros de red obteniéndolos de un servidor.

- Protocolo DNS, que es un protocolo que traduce entre nombres y direcciones IP para que podamos hacer referencia a un host de la interred por un nombre en vez de por una dirección IP.

De entre los protocolos de aplicación destacamos los siguientes:

- Protocolo HTTP, que es el que utilizan navegador y servidor Web para comunicarse.

- Protocolo FTP, utilizado para la transferencia de ficheros.

- Protocolo SMTP, utilizado para el envío de correo.

- Protocolo POP, utilizado para la descarga de correo.

- Protocolo Telnet, utilizado para el inicio de sesiones remotas en otros equipos.

7. Redes (III)

Origen de internet

Internet es una interred pública y de ámbito mundial, en la que los equipos utilizan la pila de protocolos TCP/IP para comunicarse. Podemos datar la aparición de Internet en los años 60, en plena guerra fría, en el ámbito militar. En este contexto histórico de alta tensión, el gobierno estadounidense buscaba una forma de asegurar el mantenimiento de las comunicaciones entre distintos puntos vitales de la nación. El nuevo sistema de comunicación debía de cumplir los siguientes requerimientos: la eliminación de cualquier "autoridad central", cada máquina conectada debería tener el mismo estatus y la misma capacidad para mandar y recibir información, el envío de los datos debería descansar en un mecanismo que pudiera manejar la destrucción parcial de la Red y lo importante no debía ser la ruta que siguiese la información desde el origen al destino, sino que ésta llegara a su destino. En 1969 se construye la red ARPANET que estaba formada por sólo 4 ordenadores, otros muchos fueron añadiéndose paulatinamente a la estructura durante los siguientes años, y no todos ellos del ámbito militar, sino también del ámbito académico. Durante la década de 1970 habían surgido varios protocolos para su uso en ARPANET pero no eran compatibles. Este proceso culminó con la invención del modelo y pila de protocolos TCP/IP, al que se migró finalmente en enero de 1983. En este mismo año de 1983 la motivación de ARPANET se vuelve exclusivamente científica y académica, cuando se produce la separación de su segmento militar, el cual decide construir su propia red independiente, llamada MILNET.

En **1984** la Fundación Nacional para las Ciencias de Estados Unidos, NFS, viendo las posibilidades que ofrecía una red como ARPANET y viendo su enorme impacto, se lanzó a la construcción de una red similar que pudiera estar abierta a todos los grupos de investigación de las universidades. La red se llamó **red NSFNET.** Durante la década de **1990**, muchos otros países también construyeron redes nacionales de investigación, con frecuencia siguiendo el patrón de ARPANET y NFSNET. Éstas incluían, por ejemplo, a EuropaNET y EBONE en Europa. La RedIRIS, que desde enero de 1994 está gestionada por el Consejo Superior de Investigaciones Científicas, fue el motor de conexión de ordenadores y formación de personas en España. Con la interconexión de todas estas redes con NFSNET, nace la red mundial de comunicaciones que hoy conocemos con el nombre de **red INTERNET**.

Entre 1970 y 1990, Internet y sus predecesores tenían **cuatro aplicaciones principales**: correo electrónico, noticias, inicio remoto de sesión y transferencia de archivos.

En **1992** una nueva aplicación, la **World Wide Web** o **telaraña mundial** cambió todo esto, atrayendo a millones de nuevos usuarios no académicos a la red.

Redes Privadas

En una interred sin comunicación con el exterior, su propietario asigna las direcciones IP que desee, siempre que no haya dos equipos con la misma. Sin embargo, **en una interred pública como Internet no puede permitirse una asignación desordenada de direcciones**, porque esto nos llevaría a una duplicidad de direcciones. Para evitarlo, en Internet existe un **organismo que** es el que **controla y gestiona la asignación de direcciones**:

- Hasta 1998 dicho organismo era el **IANA** (Internet Assigned Number Authority) o Autoridad para la asignación de direcciones IP.

- Posteriormente dicha labor pasó a manos del **ICANN** (Internet Corporation for Assigned Names and Numbers) u Organización de Internet para la asignación de direcciones IP y nombres de dominio.

No obstante, debido a las dimensiones y al carácter mundial que ha adquirido Internet, **la gestión y asignación de los recursos se han delegado en ciertas autoridades regionales, llamados RIRs** (Regional Internet Registries) **o Registros Regionales de Internet**, encargándose el ICANN de las tareas de coordinación entre ellos. Así, el ICANN ha asignado grandes bloques de direcciones IP a cada uno de los distintos RIRs, los cuales se encargan de su reparto real. Actualmente hay cinco Registros Regionales de Internet:

- AfriNIC, que se encarga de la región formada por África.
- APNIC, que se encarga de la región formada por el Pacífico Asiático.
- ARIN, que se encarga de la región formada por Norteamérica.
- LACNIC, que se encarga de la región formada por Latinoamérica y El Caribe.
- RIPE NCC, que se encarga de la región formada por **Europa**, Oriente Medio y parte de Asia Central.

Si una empresa privada situada en España quisiese conectar su red a Internet tendría que:

- pedir a la organización RIPE NCC que le otorgase la propiedad de una dirección (identificador) de red
- y tendría que adaptar las direcciones de sus equipos a dicha red.
- Si nuestra red tuviese menos de 254 equipos tendríamos que solicitar la asignación de una red de tipo C.
- Si fuese mayor, tendríamos que pedir una red de tipo B o A.

El problema es el agotamiento de las direcciones que es el principal motivo para la migración al protocolo IPv6. Si no podemos asignar una red a nuestra organización se soluciona mediante lo que se conoce con el nombre de **red privada**. Una red privada es definida como una red basada en la pila de protocolos TCP/IP pero de titularidad privada. Dentro del espectro de direcciones de redes posibles, existe un conjunto de ellas que se ha decidido que no sean válidas en Internet y que sean reservadas para un propósito especial: ser utilizadas solamente dentro de redes privadas. Estas direcciones son las siguientes:

- Clase A: 10.0.0.0
- Clase B: 172.16.0.0 – 173.31.0.0
- Clase C: 192.168.0.0 - 192.168.255.0

Como podemos apreciar, se reservan: 1 red de tipo A, 16 redes de tipo B y 256 redes de tipo C. **Estas direcciones no tienen validez en Internet**, es decir: ninguna red conectada a Internet las tendrá asignada, ningún paquete que circule por Internet podrá llevar una dirección perteneciente a estas redes como dirección de origen o destino del paquete y los routers de Internet no saben encaminar los paquetes hacia ellas porque no pueden tener entradas en sus tablas asociadas a dichas direcciones. Estas direcciones han sido reservadas para que sean asignadas a **redes privadas**. Está **es la única manera de poder conectar la red privada a Internet,** si se usan otras direcciones la red privada no podrá conectarse a Internet.

Protocolo NAT

¿Cómo vamos a poder conectar una red privada a Internet si dicha red privada está usando direcciones que no son válidas en Internet? Para solucionar este problema se utiliza un router provisto de un protocolo especial: el protocolo NAT, Network Address Translation o traducción de direcciones de red. Este router, que recibe asimismo el nombre de router NAT:

- Estará **conectado tanto a Internet como a la interred privada**. Por lo tanto, tendrá una dirección IP de Internet válida, llamada IP pública, y una dirección IP dentro de la red privada, llamada IP privada.
- Será el **router de salida a Internet de toda la interred privada**.
- Será el **único equipo que existe para el resto de Internet**.
- Será el **representante de cara a Internet de todos los equipos de la red privada**. La máquina de Internet que recibe la conexión lo hace desde la dirección pública del router NAT y no sabe nada de la existencia de una red privada detrás del router.
- Su **conexión a Internet** será **compartida** por todos los equipos de la red privada.

El proceso es el siguiente:

- El equipo de la red privada lanza la conexión al ordenador de Internet como lo haría en cualquier otra situación. Es decir, los paquetes IP tendrán como dirección IP de origen la del equipo de la red privada y como dirección IP de destino la del ordenador de Internet al que se quiere conectar.
- Este tráfico, para salir de la interred privada tiene que pasar por el router NAT, pues es el que da conectividad hacia Internet.
- El router sustituirá entonces la dirección IP de origen de los paquetes por su dirección IP pública. Por lo tanto, será el router NAT el que se conecte a la máquina destino de Internet. De hecho, la máquina de Internet que recibe la conexión lo hace desde la dirección pública del router NAT y no sabe nada de la existencia de una red privada detrás del router.
- El ordenador de Internet que recibe la conexión dirigirá el tráfico de respuesta al router NAT, pues es el que a ha establecido la comunicación con él a todos los efectos.
- Evidentemente, el router NAT tiene la información y los mecanismos necesarios para saber a qué equipo interno de la red privada está representando en cada comunicación abierta y poder así redirigirles este tráfico de respuesta.

Conexión a internet

Un proveedor de servicios y acceso a Internet es una **empresa que proporciona acceso a Internet a sus clientes, ya sean empresas o particulares, a cambio del pago de una cuota mensual**. Un ISP hace las funciones de distribuidor, revendiendo a sus clientes la capacidad de acceso a Internet que él mismo ha contratado a un operador de comunicaciones. Generalmente, los propios operadores de telecomunicaciones suelen ser al mismo tiempo los proveedores de acceso a Internet, con lo que ambos términos acaban confundiéndose, pero un ISP no tiene por qué ser obligatoriamente un operador de telecomunicaciones.

En este esquema de conexión a Internet a través de un proveedor de servicios, se presentan dos tramos bien diferenciados:

- **El acceso local, bucle local o red de acceso** es el tramo de la conexión que une el domicilio de los usuarios finales con la central del proveedor de Internet.
    - Si el ISP es un operador de telecomunicaciones, este tramo de la conexión será a través de una red de comunicaciones perteneciente a dicho operador; por ejemplo, una red de fibra óptica o la red telefónica básica

    - Si el ISP no es un operador de telecomunicaciones, este tramo de la conexión será a través de la red de comunicaciones de algún operador de telecomunicaciones al que el ISP haya alquilado su utilización.

- **La red de tránsito**, es el tramo de la conexión que va desde la central del proveedor de servicio a algún nodo de la red de datos IP llamada Internet, dando conectividad a la misma.

Una vez que hemos contratado una conexión a Internet a algún proveedor, ya podremos:

- Dar acceso a Internet a un ordenador individual, que utilizará dicha conexión a Internet.
- Dar acceso a Internet a toda una red privada que compartirá la conexión a Internet contratada siguiendo el esquema que se analizó en el apartado anterior.

De cualquiera de las dos formas, nuestra salida a Internet será a través de nuestro ISP, el cual tendrá que asignarnos una dirección IP pública. Generalmente, cada ISP tiene un grupo de direcciones IP públicas asignadas y las distribuye entre sus clientes, ya sea mediante una asignación estática de direcciones o mediante una asignación dinámica de direcciones. Nuestra elección del ISP será mediante dos criterios básicos:

- **Velocidad de la conexión**. La velocidad de conexión hace referencia a la **cantidad de información que puede ser transmitida por unidad de tiempo** en el tramo de la conexión entre el usuario final y su proveedor de acceso a Internet; es decir, **en el bucle local**. En la mayoría de las ocasiones dicha **velocidad es asimétrica**; es decir, la velocidad de subida es distinta a la velocidad de bajada.
- **Precio de la conexión.** El precio de una conexión dependerá fundamentalmente de la velocidad de conexión que se contrate.

Conexión a través de la Red Telefónica Conmutada (RTC) o Red Telefónica Básica (RTB):

- conexión más común entre los primeros usuarios de Internet,
- tecnología lenta, de velocidad asimétrica (máxima de bajada de 56 Kbps, y una velocidad teórica máxima de subida de 33'6 Kbps),
- uso del par de cobre como medio de transmisión.
- Es conocido con el sobrenombre de conexión dial-up, pues la conexión no es permanente, sino que se establece en el instante mediante una llamada telefónica al número proporcionado por el ISP.
- Los datos tienen que ser transformados de analógicos a digitales de lo cual se encarga un periférico llamado módem.

Conexión ADSL o Línea de Abonado Digital Asimétrica

- Es una tecnología de acceso de las llamadas de banda ancha o de alta velocidad, velocidad es asimétrica
- Utiliza el mismo cableado de par de cobre del teléfono analógico para la transmisión de datos a alta velocidad pero se puede estar usando el teléfono al mismo tiempo que se está conectado a Internet mediante ADSL.
- Se trata de una conexión permanente

- Utiliza para la transmisión a través del medio un periférico llamado módem ADSL.
- no todas las líneas telefónicas pueden ofrecer este servicio

Conexión por cable

- Utiliza la infraestructura de la Televisión por Cable (CATV)
- Utiliza una red de las llamadas híbridas, pues está compuesta por dos medios de transmisión distintos: **fibra óptica** en el corazón de la red, y **cable coaxial** en el tramo final que llega a nuestras casas.
- tecnologías de acceso de alta velocidad o banda ancha con velocidad asimétrica
- conexión permanente
- Utiliza para la transmisión a través de un periférico llamado **cablemódem** o **módem de cable**.
- Tiene como principal freno a su expansión que **es necesario desplegar una red de acceso completamente nueva**

Otras tecnologías de acceso

Actualmente están empezando a aparecer operadores que ofrecen acceso a Internet a través de tecnologías novedosas, entre las que destacamos las dos siguientes:

- **Conexión inalámbrica**. La tecnología inalámbrica, **sin cables**, ha irrumpido recientemente con fuerza gracias a la comodidad y **libertad de movimiento.** Ya hay varios operadores en ciertos núcleos urbanos, llamados **WISP** (Wireless Internet Service Provider) o **Proveedores de Acceso Inalámbrico a Internet**, que ofrecen conexión a Internet. Dichos operadores están desplegando la infraestructura necesaria, unas antenas llamadas **puntos de acceso**, que permitan disponer de un **bucle local inalámbrico**
- **Conexión a través de la red eléctrica**. Todavía en fase de pruebas, se espera que el futuro del acceso a Internet esté en el uso la red eléctrica como bucle local, con lo que se conoce como **tecnología PLC** (Power Line Communication) o **tecnología para la comunicación a través de la línea eléctrica**. La gran ventaja que ofrece es que la red eléctrica ya está desplegada y llega a todos los lugares

Protocolos de infraestructura TCP/IP

Dentro de los protocolos de nivel de aplicación existen unos cuantos que no tienen como finalidad definir la comunicación entre dos aplicaciones de usuario, sino que son protocolos que facilitan a los usuarios el uso de la red. Estos protocolos reciben el nombre de protocolos de infraestructura TCP/IP, y en los siguientes apartados vamos a analizar brevemente los dos más importantes: el protocolo o servicio DHCP y el protocolo o servicio DNS.

Servicio DHCP

Es un protocolo para la Configuración Dinámica de Equipos, y define cómo conseguir una gestión centralizada y automatizada de las direcciones IP de los equipos de una red. Los equipos le preguntan al servidor, en el momento de arranque, cuál es la dirección IP que deben utilizar, de esta manera, el administrador de la red no tiene que ir equipo por equipo configurando las direcciones IP de cada uno de ellos, sino que esta tarea puede realizarla en el propio servidor

DHCP.

- Puede establecer que a cada ordenador se le asigne una dirección IP de manera aleatoria de entre las que haya disponibles en ese momento.
- Puede establecer que a cada ordenador, identificado por la dirección MAC de su tarjeta de red, se le asigne siempre la misma dirección IP.
- Puede establecer rangos de direcciones asignables y no asignables.
- Puede establecer la duración que tiene la asignación de dicha dirección IP pasada la cual el ordenador deberá negociar su renovación.

El protocolo DHCP también dá la siguiente información: la máscara de subred que tienen que utilizar, cuál es la dirección del router que les da salida fuera de la subred y la dirección del servidor DNS que tienen que utilizar.

Para establecer la comunicación el protocolo establece que el cliente debe usar la dirección IP 0.0.0.0 como dirección origen y la dirección IP 255.255.255.255 como dirección destino

Servicio DNS (Domain Name System)

O Sistema de Nombres de Dominio, y cuya misión es la de hacer de traductor entre direcciones IP y nombres de dominio, proceso que recibe el nombre técnico de resolución de nombres.

El sistema es:

- **Un sistema distribuido.** La información de traducción no debía estar centralizada en un único ordenador. También para acelerar la búsqueda en la tabla lo que debía hacerse era partir la tabla de traducción de nombres en varias partes y distribuir éstas entre distintos ordenadores, de tal manera que cada uno de ellos manejase sólo una parte de la tabla
- **Un sistema jerárquico**. No debía haber un único organismo que controlase y gestionase la asignación de los nombres a los ordenadores, sino que se necesitaba una estructura más flexible que pudiese dar respuesta y adaptarse al dinamismo que caracteriza a Internet. Lo que debía hacerse era crear una organización en la que se delegasen las competencias en distintas autoridades que fuesen capaces de autogestionarse, aunque estuviesen supervisadas por una autoridad superior.

Existe un nodo raíz de la estructura. Del nodo raíz surgen una serie de hijos, llamados dominios de primer nivel o simplemente dominios (com, net, org, etc) donde cada uno de ellos tiene capacidad de autogestión. Cada dominio tiene potestad para decidir dividirse a su vez en unidades más pequeñas con capacidad de autogestión, llamadas subdominios.

Ejemplo: "**www.juntadeandalucia.es**"

- El nombre del dominio de **primer nivel**, o simplemente dominio, al que pertenece el ordenador. En este caso al dominio ".es"; es decir, es un ordenador que pertenece al dominio administrado por España.
- El nombre del **subdominio**, dentro del dominio ".es", al que pertenece el ordenador. En este caso al subdominio "juntadeandalucia"; es decir, al subdominio que España ha delegado a la Junta de Andalucía para que lo administre como desee.
- El nombre del ordenador dentro del subdominio juntadeandalucia. En este caso el ordenador tiene el nombre de "WWW"; que es el nombre que la Junta de Andalucía ha

decidido poner a ese ordenador.

La única condición que se impone es que no otorgue dos veces el mismo nombre. El proceso de resolución de nombres de dominio lo realiza el servidor de nombres o servidor DNS. Todo ordenador conectado a Internet debe conocer la IP de al menos uno. **Un servidor de nombres es un ordenador, o más correctamente dicho, una aplicación ejecutándose en un ordenador, que tiene asignadas las siguientes dos tareas**:

- Aceptar y atender peticiones de usuarios que le solicitan que les convierta un nombre de dominio en su dirección IP asociada.
- Aceptar y atender peticiones de otros servidores de nombres que le solicitan que les convierta un nombre de dominio en su dirección IP asociada.

Cuando un servidor de nombres recibe una petición puede hacer cuatro cosas:

- Responder directamente a la petición si es que ya conoce cuál es la dirección IP
- Puede contactar con otro servidor de nombres para tratar de averiguarla
- Puede responder algo así como: "No conozco la dirección IP asociada al nombre de dominio que me pides, pero te voy a facilitar la dirección IP de otro servidor DNS que sabe más de lo que yo sé".
- Puede responder con un mensaje de error porque el nombre de dominio que debe resolver no es válido o no existe.

Servicios en internet

Son las aplicaciones o servicios de Internet que utilizan directamente los usuarios para alcanzar sus fines. La mayoría de estos protocolos de aplicación, aunque no todos, siguen lo que se conoce como modelo cliente-servidor. En el modelo de comunicación cliente-servidor, de las dos aplicaciones involucradas en la comunicación hay una que es la que ofrece el servicio, y recibe el nombre de servidor, y hay otra es la que solicita el servicio, y recibe el nombre de cliente.

- El **cliente** es una aplicación que usando las reglas establecidas en el protocolo de aplicación que esté utilizando, ejecuta peticiones que son enviadas a través de la red a la aplicación servidora.
- El **servidor** o aplicación servidora permanece a la escucha en un puerto del ordenador a través del cual le irán llegando dichas peticiones. Entonces, la aplicación servidora realizará las tareas necesarias para servirlas y responderá al cliente con los resultados. Podemos observar que en este modelo el cliente es el que lleva la iniciativa en cada solicitud, mientras que el servidor se limita a seguir las órdenes cursadas por el cliente.

Los servicios que se ofrecen en Internet son muy variados, pero los cuatro más importantes son los siguientes: servicio Web, servicio de correo electrónico, servicio de transferencia de archivos y servicio de inicio remoto de sesión.

Servicio Web

A finales de los años 80 Internet había alcanzado ya un tamaño considerable y el volumen de información aunque era **caótico** y desordenado siendo una red de uso complejo sólo apta para investigadores y técnicos. Se vio entonces la necesidad de llegar a un acuerdo para almacenar la información en un formato común, que permitiese un acceso homogéneo. A principios de los 90 **nace** en el seno del CERN (**C**onseil **E**uropéen pour la **R**echerche **N**ucléaire) o **Consejo Europeo para la Investigación Nuclear**, y de manos de Tim Berners Lee, la **World Wide Web**, la telaraña mundial o simplemente la Web. Este nuevo servicio de Internet recibió el nombre de servicio Web;

su misión: proporcionar a los usuarios la capacidad de consultar información alojada en otros ordenadores en formato de páginas electrónicas o páginas Web

- **Arquitectura del servicio Web:** sigue el modelo cliente-servidor
    - El servidor. En el servicio Web, la aplicación recibe el nombre de Servidor Web, y su misión es la de poner a disposición de los clientes una serie de recursos.
    - El cliente. La aplicación que desempeña el papel de cliente recibe el nombre de Navegador Web, y su misión es la de solicitar al servidor la entrega de alguno de los recursos que ofrece.

  Las reglas que rigen una comunicación Web entre un navegador y un servidor Web, vienen recogidas en un protocolo de nivel de aplicación llamado HTTP (HyperText Transport Protocol). El hipertexto es un documento digital que se puede leer de manera no secuencial compuesto por texto e hiperenlaces. Se llama recurso a cualquier fichero alojado en un servidor y accesible por los clientes haciendo uso del protocolo adecuado
- **Dirección Web o URL:** forma de identificar un recurso de manera unívoca en toda la Red. Para ello se utiliza la URL (Uniform Resource Locator) o Localizador Uniforme de Recursos. La URL está formada por el protocolo seguido de "://", luego la localización en Internet de la aplicación servidor Web en la que se encuentra el recurso buscado y la localización en el servidor Web del recurso
- **El recurso por excelencia:** la página Web: es Una página Web es un fichero de texto, generalmente con extensión .htm o .html, que se encuentra escrito en un lenguaje llamado HTML (HyperText Markup Language) o Lenguaje de Marcado de Hipertexto (su misión es la de indicarle al navegador cómo debe presentar los contenidos que componen la página). Aparte puede incluir referencias a otros recursos como imágenes, animaciones, etc.
- **Seguridad en la Web:** HTTPS es un protocolo que permite la transmisión segura de información entre el navegador y el servidor Web mediante el uso de mecanismos de cifrado y certificados de autentificación.

Servicio de Correo Electrónico

Un correo electrónico o email, no es más que un simple mensaje de texto; es decir, un trozo de texto enviado a un destinatario. El servicio de correo electrónico proporciona a los usuarios cinco funciones básicas:

- **Función de composición**. El sistema de correo electrónico debe permitir al usuario crear sus propios mensajes de correo y generar mensajes de respuesta a los correos recibidos.
- **Función de transferencia**. El sistema de correo electrónico tiene que mover los mensajes del emisor al destinatario y debe hacerlo automáticamente, sin molestar al usuario.
- **Función de generación de informe**. El sistema de correo debe indicar al remitente lo que ocurrió con el mensaje: ¿se entregó, se rechazó o se perdió?
- **Función de visualización**. El sistema de correo debe permitir al usuario ver y leer el contenido de los correos que le sean entregados.
- **Función de disposición**. El sistema de correo debe permitir al usuario decidir qué hace con los correos entrantes tras recibirlos. Las posibilidades suelen incluir las de tirarlo antes de leerlo, desecharlo tras leerlo, guardarlo, etc. También debe permitir recuperar y releer mensajes previamente guardados, reenviarlos o procesarlos de otras maneras.

A continuación se describe el servicio:

- **Arquitectura del servicio de correo electrónico:** sigue la filosofía cliente-servidor; sin embargo, su arquitectura es un poco más compleja que la de otros servicios de Internet. Se llama clientes de correo o agentes de usuario a los programas utilizados por los

usuarios finales y que les permiten: leer, componer, recibir, contestar y enviar correo. El servidor de correo es una aplicación que tiene básicamente dos compromisos adquiridos con los usuarios a los que da servicio: Mantener buzones para dichos usuarios y almacenar en ellos los correos que les van dirigidos y recoger los correos que los usuarios a los que da servicio le envían y encargarse de que estos lleguen hasta el buzón del destinatario. Un ordenador que hace de servidor de correo realmente está ejecutando dos aplicaciones servidoras diferentes:

- Una recibe el nombre de **servidor saliente o servidor SMTP** (puerto 25) es el protocolo que se utiliza para el envío de correo
- La otra recibe el nombre de **servidor entrante** y tendrá la misión de gestionar la entrega del correo al usuario final al que va destinado. **Hay dos protocolos básicos que pueden ser utilizados para llevar a cabo esta tarea.**
    - Uno de ellos es el **protocolo POP3** (Post Office Protocol) o **Protocolo de Oficina de Correos, versión 3** (puerto 110)
    - El otro es el **protocolo IMAP** (Internet Mail Access Protocol) o **Protocolo para el Acceso al Correo Electrónico** (puerto 143)

- **Direcciones de correo electrónico:** Nombre del buzón de correo dentro del servidor, un símbolo separador, que se ha decidido que sea la arroba: @ y el nombre DNS del ordenador en el que se encuentra la aplicación servidor de correo.
- **Formato de un mensaje de correo electrónico:** En todo mensaje de correo podemos distinguir las siguientes partes:
    - La envoltura primitiva, la cual encapsula al mensaje y contiene toda la información que necesitan los agentes de transferencia de correo (MTA) para poder transportarlo desde el servidor origen hasta el servidor destino. Sería como el sobre en el correo tradicional y es transparente para el usuario.
    - Cabecera del mensaje contiene información de control para los clientes de correo. Formada por un número variable de campos, aunque algunos son obligatorios. Destacamos:
        - **Campo Para.**
        - **Campo De**.
        - **Campo CC** o campo de copia al carbón. Campo que contiene las direcciones de correo de aquellos destinatarios del mensaje a los que, aunque el correo no va dirigido a ellos, se les quiere mandar una copia del mismo. Estos reciben el nombre de destinatarios secundarios y, en términos de entrega, no hay diferencia entre ellos y los destinatarios primarios. Es una diferencia por entero sicológica que puede ser importante para los participantes, pero que no lo es para el sistema de correo.
        - **Campo BCC** o campo de copia de carbón ciega. Campo similar al campo CC, excepto que esta línea se borra de todas las copias enviadas a los destinatarios primarios y secundarios. Esta característica permite a la gente mandar copias a terceros sin que los destinatarios primarios y secundarios lo sepan.
        - **Campo Asunto**.
        - **Campo Fecha**. Campo que contiene la fecha y hora del envío del mensaje.
        - **Campo Responder a**. Campo que contiene la dirección de correo a la que deben enviarse las contestaciones al mismo. Generalmente contiene el mismo valor que el campo De

    - Cuerpo del mensaje. Dentro de lo que es el mensaje en sí

- **Seguridad en el correo electrónico:** Muchos servidores de correo ofrecen la posibilidad de utilizar protocolos seguros para la transmisión del correo entre el cliente de correo y el servidor, ya sea en el proceso de envío de mensajes o en el proceso de recogida de correo desde el buzón. Estos protocolos siguen siendo SMTP y POP3 o IMAP, pero utilizando protocolos de cifrado, como SSL o TLS, antes de enviar la información. El uso de estos protocolos asegura:
    - Que si el correo es interceptado durante la transmisión entre cliente de correo y servidor de correo, no podrá ser leído.
    - Que el correo no podrá ser modificado durante la transmisión entre cliente de correo y servidor.

  Aunque no garantizar la completa privacidad del correo. Para garantizar de manera total la seguridad en las comunicaciones por correo electrónico, debemos recurrir a sistemas criptográficos extremo a extremo. Uno de estos sistemas es PGP

Servicio de Transferencia de Archivos

Permite a los usuarios copiar archivos entre sistemas remotos. Sigue la filosofía cliente-servidor. Existen dos tipos de aplicaciones implicadas:

- El **servidor FTP**. El servidor FTP es la aplicación que aporta el servicio de proporcionar un espacio de disco en el que se puedan dejar archivos o desde el que se puedan recoger archivos.
- El **cliente FTP**. El cliente FTP es la aplicación que permite a un usuario conectarse a un servidor FTP para poder dejar en él algún archivo o para poder descargar de él algún archivo.

FTP se configura para autentificar los inicios de sesión de los clientes, pidiendo login y password, antes de acceder al sistema. Sin embargo, esta autentificación no es obligatoria siempre. FTP tiene dos modalidades de uso:

- **FTP Anónimo**: Esto supone un servidor FTP configurado para permitir el acceso público. En unas ocasiones sólo se pueden descargar ficheros, y en otras éstos se pueden tanto subir como bajar.
- **FTP Privado**: En este caso el servidor se basa en autentificación a partir de la base de datos de usuarios locales, por lo tanto, sólo pueden iniciar sesión los usuarios que hayan sido dados de alta en dicho sistema.

Cuando se establece una sesión FTP entre un cliente y un servidor, realmente se establecen dos conexiones con el servidor:

- **Una conexión de control**, que es iniciada por la aplicación cliente para la transmisión de comandos a través del puerto 21 del servidor, y que es mantenida durante toda la sesión.

- **Una conexión de datos**, que es iniciada por la aplicación servidora para la transmisión de datos, y que se abre y se cierra por archivo a enviar o recibir. Cada una de estas conexiones temporales se abre desde el puerto 20 del servidor contra un puerto cualquiera del cliente que éste le haya comunicado previamente.

Servicio de Conexión remota

Los servicios de conexión remota siguen la filosofía cliente-servidor:

- El servidor, el cual es, desde el punto de vista del usuario del servicio, el ordenador remoto en el cual se abre la sesión del sistema operativo y sobre el cual se trabaja.
- El cliente, el cual es, desde el punto de vista del usuario, el ordenador local desde el cual se abre la sesión en el ordenador remoto.

Podemos distinguir dos tipos de servicios:

- Conexión remota con **terminal de comandos.** Cabe destacar el protocolo originario, llamado Telnet, que es un protocolo para la conexión remota con terminal de comandos. Sin embargo, aunque establece mecanismos para la autenticación del usuario que quiere abrir la sesión mediante el requerimiento de un login y un password, es considerado un protocolo no seguro. Por otra parte, existe otro protocolo muy parecido que sí es seguro, pues utiliza técnicas de cifrado para que la información que viaja por la red no pueda ser leída por nadie al que no vaya dirigida. Dicho protocolo es el protocolo SSH (Secure shell) o terminal de comandos seguro.
- Conexión remota con **terminal gráfico.**

Mecanismos de seguridas básicos en internet

Un virus es un programa cuyo objetivo prioritario es su propagación entre ordenadores sin ser advertido por el usuario. Una vez que el virus considera que está lo suficientemente extendido**,** pasa de su fase de latencia a su fase de activación. En esta fase los efectos del virus pueden ser tan variados como alcance la imaginación de su autor: pueden limitarse a mostrar inofensivos mensajes en pantalla o bien, eliminar información del disco duro o dañar la BIOS del ordenador. La principal vía de infección de virus son las redes de ordenadores, y dentro de los servicios que ésta ofrece, el favorito usado por los virus para su propagación es el correo electrónico. Distinguimos dos tipos de virus:

- **Los gusanos**. Se llama gusanos a los virus que usan para replicarse las redes de ordenadores y los agujeros de seguridad de los programas instalados en los ordenadores de las mismas. Una vez que un virus gusano ha infectado un ordenador, estudia la red en busca de alguna otra máquina que tenga instalado y funcionando el software que tiene el agujero de seguridad que dicho gusano explota. Entonces, se copia vuelve a copiar a sí mismo en el nuevo ordenador y comienza de nuevo su proceso de réplica.
- **Un caballo de Troya** es un programa que tiene una apariencia inofensiva pero que realmente tiene objetivos hostiles. Se trata de un programa con dos módulos: un módulo servidor y otro cliente.

Nos podemos proteger de dos formas:

- Mediante el uso de programas antivirus, los cuales detectan la presencia de virus en archivos impidiendo la infección del sistema.
- Mediante una adecuada formación de los usuarios.

Los antivirus no son los programas más efectivos para enfrentarse a los caballos de Troya. En su lugar, es más recomendable la utilización de un firewall o cortafuegos, ya que éstos pueden impedir que una aplicación de este tipo se comunique a través de la red. Un cortafuegos es una herramienta hardware o software utilizada en las redes de ordenadores con el objetivo de dotar de cierta seguridad a las mismas. La decisión de si un paquete IP puede pasar el firewall o no se tomará en función de las direcciones IP origen y/o destino de dicho paquete, así como del puerto

origen y/o destino al que vaya dirigida la información que dicho paquete transporta. Así, por ejemplo, con un firewall:

- Se puede impedir el paso a todo el tráfico IP que vaya dirigido a una cierta dirección IP o a una red concreta.
- Se puede impedir el paso a todo el tráfico que provenga de cierta dirección IP o de cierta red concreta.
- Se puede impedir el paso a todo tráfico que no provenga de cierta dirección IP o de cierta red concreta o que no vaya dirigido a cierta dirección IP o a cierta red concreta.
- Se puede impedir el paso del tráfico que vaya dirigido a un puerto concreto
- Se puede permitir el acceso al puerto 80 de ciertos ordenadores e impedir el acceso al puerto 80 de otros ordenadores, con lo que estableceríamos a qué servidores Web nos podemos conectar y a cuáles no.
- Se puede, en definitiva, hacer cualquier combinación de criterios que juegue con direcciones IP origen y destino de los paquetes y puertos origen y destino de la información que transportan.

Podemos distinguir dos tipos de firewall:

- **Cortafuegos corporativos**. Es un firewall hardware o software **situado en el router de salida o entrada de una red** local y cuyo objetivo es el de dar protección a la misma, controlando qué tráfico puede salir y entrar desde y hacia la red.
- **Cortafuegos personales**. Es un firewall software **situado en un ordenador personal** y cuyo objetivo es el de dar protección al mismo

Un servidor proxy HTTP es una aplicación que se sitúa entre el navegador y el servidor Web de tal manera que intercepta las conexiones HTTP de aquél y lo sustituye de cara al servidor. Al pasar todas las conexiones HTTP a través de esta aplicación, se pueden establecer en ella ciertos criterios de filtrado para controlar, en función de la URL solicitada, qué conexiones HTTP están permitidas y cuáles no. Así, por ejemplo:

- Se pueden impedir las conexiones a ciertas URLs, explicitando cuáles deben ser restringidas.
- Se puede afinar aún más en este aspecto, impidiendo las conexiones a URLs que contengan alguna palabra clave, por ejemplo, la palabra sexo.
- Se puede impedir la descarga de recursos de un cierto tipo, por ejemplo, fotos o ficheros musicales.

Generalmente el servidor **proxy HTTP** se sitúa, al igual que el cortafuegos, en el router de salida de la red. También podemos realizar las siguientes acciones:

- Se puede mantener un registro de quién está navegando por la Web, cuándo se conecta y dónde se conecta.
- Se pueden establecer horas en las que la conexión esté permitida y horas a las que no.
- Se pueden especificar distintas políticas de uso de la Web, de tal manera que unos usuarios tengan unas restricciones y otros usuarios tengan otras o ninguna.
- Se puede acelerar el acceso a la Web mediante el uso de una caché en el servidor proxy. Si esta opción de configuración del servidor proxy está disponible y activada, el servidor mantendrá una copia de las páginas solicitadas, de tal manera que si vuelven a ser pedidas posteriormente, por el mismo o por otro usuario, éstas pueden ser servidas por el proxy en vez de por el servidor que aloja dichas páginas realmente, lo cual se traduce en una mayor rapidez de servicio.
- Se puede compartir la conexión a Internet para la navegación Web. Si sólo tiene conexión a Internet un único ordenador, por ejemplo, mediante una conexión ADSL, el resto de ordenadores de la red local pueden navegar por la Web a través de él si dicho ordenador cuenta con una aplicación proxy HTTP que los sustituya en las conexiones.

8. Linux (I)

¿Qué es Linux?

En 1987 el profesor Andrew S. Tanenbaum escribió un libro sobre diseño de sistemas operativos. Como parte de ese libro escribió un sistema operativo sencillo que se llamó Minix y simulaba a UNIX. Uno de los seguidores de Minix se llamaba Linus Torvalds, un estudiante de informática finlandés. Torvalds decidió modificar Minix para utilizar las características del microprocesador 80386 de Intel que en el futuro constituyó lo que hoy conocemos como Linux, un clónico de UNIX con licencia GNU. El software distribuido bajo licencia GNU puede ser modificado y vuelto a distribuir siempre que se acompañe del código fuente, además de otras condiciones. Pero lo importante es que siempre se acompaña el código fuente, esto hace que un programador pueda continuar o perfeccionar el trabajo de otro. Esto se conoce como software libre.

Tipos de software por su licencia de uso

- **Software comercial:** El desarrollado por una empresa con intención de venderlo. Hay que aclarar que un software puede ser libre y al mismo tiempo comercial, como por ejemplo el sistema gestor de bases de datos *MySQL.* El cual, aunque es software libre, dependiendo del uso al que se destine puede ser comercial.
- **Software libre:** El que puede ser distribuido, modificado, copiado y usado. No hay que confundirlo con software gratis. El matiz está en la difusión del código fuente.
- **Software semilibre:** En este caso se imponen algunas restricciones, normalmente para usarlo en entornos empresariales, mientras que para usuarios domésticos mantiene las condiciones del software libre. Un ejemplo puede ser el software de encriptación de correo electrónico PGP.
- **Software propietario:** Aquél que prohíbe su redistribución, modificación y copia. Se puede utilizar con el pago de licencias de uso a sus fabricantes. En esta categoría encontraremos a la mayor parte del software que se utiliza, en concreto a toda la familia de sistemas operativos Windows o el paquete ofimático Office de Microsoft.
- **Freeware:** Se puede utilizar libremente pero su código fuente no está disponible. Existen multitud de programas con este tipo de licencia que pueden obtenerse fácilmente desde Internet, un ejemplo puede ser el cliente de correo Pegasus Mail.
- **Shareware:** Se permite su redistribución y copia, pero no se acompaña de código fuente y además suele tener alguna limitación de uso temporal. Se utiliza para distribuir programas de forma que se puedan probar antes de comprar la licencia de uso. Un ejemplo típico podría ser el compresor de ficheros Winzip.

Distribuciones Linux

Linux sólo es el núcleo del sistema. Pero el núcleo por sí sólo no es capaz de ofrecer casi ninguna funcionalidad al usuario. El núcleo de un sistema operativo se encarga de las labores más básicas (pero muy importantes) de acceso al hardware, control de procesos, entrada/salida, etc.

Se conoce como **distribución** de Linux a la unión del kernel Linux junto con programas de aplicación que aporten funcionalidad para el usuario final, unas tienen un propósito general y otras en cambio están orientadas a una labor muy concreta

Guadalinex

Guadalinex ofrece un interface de usuario en modo gráfico basado en el concepto de escritorio. Se pueden utilizar escritorios diferentes ya que el escritorio es una parte separada del núcleo del sistema. Guadalinex usa Gnome.

Hay que destacar que por debajo de los escritorios y antes de llegar al núcleo o kernel del sistema existe un paso intermedio que es el manejador de gráficos de Linux, éste se llama **X Windows** y son las rutinas básicas para hacer funcionar la tarjeta de video o establecer la resolución de pantalla y profundidad de color.

Características de linux

- Multiusuario: pretende garantizar la confidencialidad y seguridad de los datos almacenados.
- Usuarios y grupos: existen dos tipos de usuarios, el superusuario o *root* y todos los demás.
    - El **superusuario** será la persona que administre el sistema y tendrá derechos plenos sobre éste.
    - **El usuario *root*** se crea en la instalación de Linux y no puede borrarse, su login es root y tampoco puede cambiarse.
    - **El resto de los usuarios** tendrán **capacidades limitadas de utilización** del sistema ajustadas a su nivel de uso o requerimientos de funcionalidad. Será *root* quien asigne esas capacidades. Todos los usuarios tendrán asignado un directorio de trabajo, llamado HOME,

  Cada programa se ejecuta con los derechos del usuario que lo lanza, por eso existen unos **usuarios especiales** que se crean para que ciertos programas, normalmente servidores, se ejecuten con unos derechos concretos. Por ejemplo, cuando se instala el servidor Web Apache también se crea un usuario que en realidad no está asignado a ningún usuario humano del sistema. **Los usuarios se clasifican en grupos**, de forma que todos los usuarios de un mismo grupo pueden compartir derechos de acceso comunes a archivos y directorios.
- Linux es un sistema plenamente orientado a su utilización en red que se caracteriza por la cantidad de aplicaciones y herramientas de comunicaciones de las que dispone

Directorios, ficheros y unidades de disco

Las responsabilidades del sistema operativo son:

- la gestión de los medios de almacenamiento,
- su organización
- y puesta en servicio para los usuarios del sistema.

También hemos detallado cómo los datos se organizan en directorios (o carpetas) y se almacenan en archivos. La mayoría de las versiones de Linux actuales utilizan el sistema de ficheros Ext3, el cual incorpora muchas características de seguridad, velocidad e integridad de datos que no estaban presentes en el anterior sistema de ficheros Ext2. La más importante es que incorpora *journaling*, esto quiere decir que ante una caída o cierre no limpio del sistema la recuperación es más rápida y segura que con los sistemas anteriores.

- **Acceso a las unidades de disco:** Una característica de Linux es que para estandarizar el uso de dispositivos todos ellos son tratados como archivos, aunque en muchos casos sean archivos ficticios. Están representados por un fichero que hace referencia a ellos.

  En Linux no existe el concepto de unidad de almacenamiento, sino que ésta se hace corresponder con un archivo. El contendido de la unidad de almacenamiento será accesible a través de ese archivo. A la acción de asignar un archivo a una unidad de almacenamiento se le llama "montar" y cuando queramos dejar de utilizarla la deberemos "desmontar". Hay unidades que se montan automáticamente en el arranque del sistema y se desmontan también automáticamente en el apagado, como ocurre con la partición raíz del disco duro.
- **Estructura de directorios:** En esta jerarquía de directorios que comienza por el directorio raíz, representado por el símbolo "/", podemos encontrar, al menos, los siguientes directorios:
  - **/bin**: Contiene los ejecutables básicos del sistema operativo.
  - **/sbin**: Aquí se encuentran los ejecutables del sistema que sólo pueden ser utilizados por root o usuarios autorizados por éste.
  - **/dev**: Contiene todos los ficheros de dispositivo, de los que ya hemos hablado. Por ejemplo fd0 es la disquetera, stdin es el teclado, psaux es el ratón, hda es el primer disco duro.
  - **/boot**: Contiene los ficheros de arranque del sistema, en concreto el núcleo
  - **/etc**: Este importante directorio contiene todos los archivos de configuración del sistema, por ejemplo *hostname* contiene el nombre de nuestro ordenador, *fstab* contiene la lista de unidades que se pueden montar, *gnome* contiene la configuración del escritorio GNOME.
  - **/root**: Éste es el directorio de trabajo del superusuario *root*.
  - **/lib**: Las librerías de programación usadas por las aplicaciones.
  - **/mnt**: Aquí se suelen montar las unidades de almacenamiento.
  - **/home**: Contiene un subdirectorio por cada usuario del sistema, ese subdirectorio tiene el mismo nombre que el login del usuario que lo utiliza. Es el directorio de trabajo del usuario, también conocido como directorio HOME.
  - **/usr:** Aquí se suelen instalar las aplicaciones de la distribución.
  - **/tmp**: Un directorio de uso temporal.
  - **/var**: Directorio con los archivos logs y de trabajo de muchas de las aplicaciones instaladas.
- **Rutas y nombres de archivos y directorios:** Como es natural cada archivo o directorio debe tener un nombre único, al menos en el subdirectorio donde se encuentra. Linux distingue entre mayúsculas y minúsculas. Las rutas para designar la ubicación de un archivo o directorio se comienzan por el directorio raíz y se van enumerando los distintos subdirectorios hasta llegar al archivo deseado separándolos con el signo "/". Se puede hacer referencia al directorio actual con "." Y al directorio anterior con ".."
- **Permisos:** consiste en separar el nivel de acceso en tres grupos:
  - Permisos del usuario que creó al archivo o directorio, propietario.
  - Permisos de los usuarios del mismo grupo que el propietario.
  - Permisos del resto de usuarios.

  Para cada nivel de acceso se tienen a su vez tres tipos de permiso: Lectura (r), Escritura

(w), Ejecución (x). Hay que darse cuenta que en Linux no basta con que un programa sea ejecutable, también debemos tener permisos para su ejecución.

Un poco de teoría sobre arranque y particiones

Es imprescindible conocer qué ocurre cuando encendemos un ordenador hasta que tenemos un sistema operativo funcionando y listo para ser para ser usado. Esto se conoce como arranque del sistema o boot.

1. Encendido eléctrico: Cuando encendemos un ordenador pulsando el botón *power* del frontal estamos dando paso a la energía eléctrica hasta los circuitos de la máquina. Lo primero que ocurre es un chequeo general por el cual el propio ordenador comprueba que todos los elementos (memoria, disco, teclado, ratón, etc.) están presentes y funcionan sin problemas.
2. Búsqueda de un MBR: Si el chequeo anterior ha sido positivo, un pequeño programa almacenado en la memoria ROM del ordenador toma el control y busca algún sistema operativo que cargar en memoria. La búsqueda del sistema operativo a cargar se hace en el orden indicado en la configuración de la BIOS del ordenador (normalmente primero busca en CD, luego en disco duro, disquetera, USB). Si suponemos que el sistema operativo está en el disco duro (lo cual es la situación normal) el programa cargador de la ROM cede el control al MBR (*Master Boot Record*). Esto es una parte del disco duro que contiene la rutina de arranque del sistema operativo.
3. Ejecución del gestor de arranque: Una vez que el MBR ha tomado el control pueden ocurrir dos cosas.
    1. Si sólo hay un sistema instalado en el ordenador se comienza la carga y ejecución del mismo.
    2. Si existen varios sistemas operativos instalados se nos presentará un menú donde se nos pregunta qué sistema operativo queremos arrancar. En Guadalinex se utiliza el gestor de arranque GRUB.

En un disco duro se pueden establecer particiones de forma que cada una puede contener sistemas de archivos diferentes y sistemas operativos diferentes. Existen dos tipos de particiones:

- Partición primaria: Es arrancable y puede haber hasta 4 en un disco duro típico.
- Partición extendida: No es arrancable y contiene en su interior otras particiones que sí pueden ser arrancables con el gestor de arranque adecuado. Sólo puede haber una en un disco duro. A las divisiones internas se les llama particiones lógicas.

9. Linux (II)

Intérpretes de órdenes. Shells

Tradicionalmente se interactúa con el ordenador a través de unos **terminales** compuestos con teclado y monitor. En la actualidad el término de terminal se usa con un sentido más amplio. Aunque en un ordenador personal sólo disponemos de un terminal físico, Linux permite utilizar diferentes terminales virtuales ya que emula su función.

- podemos cambiar de un terminal a otro pulsando una determinada combinación de teclas.
- en cada uno de estos terminales puede mantenerse una sesión de trabajo distinta.
- es como si tuviéramos varios terminales físicos distintos formados por monitor, teclado, altavoz, memoria, y cable de conexión al ordenador, pero solo pudiéramos usar uno de ellos en un momento dado. Cada terminal virtual está gestionado por un controlador de dispositivo.

En una terminal de texto, debe existir una aplicación denominada intérprete de comandos (**Shell**), que traduce nuestras órdenes para que el sistema operativo pueda ejecutarlas.

Guadalinex permite trabajar con doce terminales virtuales, seis gráficas y seis de texto, accesibles desde las teclas de funcion F1 a F12 pulsando Control+Alt+Fx

La **Shell** es un programa que nos permite comunicarnos con el sistema operativo traduciendo las órdenes introducidas por el usuario a un lenguaje comprensible para el ordenador, la Shell es un intérprete de comandos. En Linux disponemos de distintos intérpretes aunque habitualmente usaremos la **Shell bash** (Bourne-Again SHell). Otras shells para Linux son Korn-Shell (ksh), Bourne-Shell (sh), C-Shell (csh). Existen también algunas para propósitos especiales: la remote-Shell (rsh) se utiliza para ejecutar comandos en un ordenador remoto y la Secure Shell (Ssh) se utiliza para establecer una conexión segura con un ordenador remoto.

Una vez identificados, el sistema queda a la espera de introducción de nuevos comandos. Para ello, se nos ofrece el **prompt** del intérprete de comandos, por ejemplo: “usuario@guadalinex:~$”. Este *prompt o indicador* es personalizable, aunque por defecto indica lo siguiente:

- el nombre del usuario registrado
- el nombre de la máquina (en este caso *guadalinex*),
- el directorio en el que estamos (el símbolo ~ representa el directorio de trabajo: /home/usuario/)
- $ indica que se trata de un usuario normal. Si el usuario fuera el administrador (*root*) el símbolo sería #

Las órdenes se escriben siguiendo la siguiente estructura y sintaxis (se distingue entre mayúsculas y minúsculas):

1. Comandos internos: Comandos que están implementados dentro de la propia Shell.
2. Comandos: Son ficheros ejecutables y por tanto deberán estar accesibles, por medio de la ruta o la variable PATH.
3. Opciones: Son letras precedidas de un signo '-' que modifican o amplían el comando.
4. Meta-caracteres y operadores de control: Son caracteres con un significado especial para la Shell, y se utilizan para complementar el resultado obtenido con los comandos.

   Ejemplo: * igual que en sistemas DOS, el comodín se sustituye por cualquier cadena de

caracteres, ? la interrogación también tiene el uso habitual, se sustituye por cualquier carácter, pero sólo uno. Otros meta-caracteres: & ; ( ) | >>

5. Argumentos: Son datos que pasamos al comando como parámetros de entrada.
6. Comentarios: Todo lo que sigue al carácter '#' hasta la nueva línea será un comentario.
7. Palabras reservadas: Son palabras reservadas para implementar el lenguaje Shell-Script que veremos más adelante. Ejemplo: case, do, done, elif, else...

Profundizamos en el uso de la Shell

Veamos algunos ejemplos sencillos de órdenes para la "Shell":

- El comando '**echo**' visualiza en pantalla todo aquello que se le pasa como argumentos.
- El comando **'ls'** muestra los archivos de un directorio.
- El comando **'date'** muestra en pantalla la fecha del sistema y el calendario.
- Comandos de manejo de directorios: cd cambia nuestro directorio, mkdir crea un directorio y pwd indica el directorio en el que estamos.
- El comando man nos da acceso al manual de Linux, y nos informa sobre la orden que le demos como argumento. Algunas operaciones básicas con man son:
    - /palabra: localiza la siguiente ocurrencia de la palabra dada como parámetro
    - ?palabra: localiza la ocurrencia anterior de la palabra dada como parámetro
    - barra espaciadora: avanza pantalla
    - q: salir
- Comando de información. who (Indica el usuario del sistema en ese momento) y whoami (indica la terminal y la sesión en que se está trabajando)
- Una facilidad que ofrece la **Shell** a la hora de introducir largos argumentos es el uso del tabulador, de manera que completa lo que estamos escribiendo

El **sistema de archivos** del sistema operativo se encarga de la administración de los datos en los dispositivos de almacenamiento. Los archivos en Linux tienen un nombre de hasta 255 caracteres y aunque no existe el concepto de extensión de un archivo es posible incluir el carácter punto "." tantas veces como se desee. No se deben incluir caracteres especiales interpretados por la Shell, como /, $, ", ', &, #, (,), *, [,], {, }, etc... Los archivos que comienzan por punto . son interpretados como archivos ocultos.

El sistema asigna un directorio personal a cada usuario. Normalmente está en /home y tiene el nombre de usuario. Se le llama también con el símbolo ~. Algunos comandos para el sistema de archivos:

- El comando **'ls'** muestra los archivos de un directorio.
- El comando **'mkdir'** crea un directorio
- El comando **'rmdir'** borra un directorio
- El comando **'cd'** cambia de directorio
- El comando **'cp'** copia un archivo a un directorio
- El comando **'mv'** mueve un archivo a un directorio
- El comando **'cat'** muestra el contenido de un archivo
- El comando **'du'** muestra el espacio usuado por el directorio
- El comando **'df'** informa del espacio usado por las particiones montadas
- El comando **'tar -cvf'** agrupa en un solo archivo tar los archivos indicados
- El comando **'tar -xpvf'** extrae un archivo del archivo tar
- El comando **'file archivo'** el sistema clasifica el archivo y muestra sus datos
- El comando **'tree'** listado recursivo
- El comando **'ln arch1 arch2**' crea un enlace para arch1 con nombre arch2.

Desde la terminal tenemos un programa que permite realizar todas estas órdenes antes descritas con un entorno más "amigable" de menús en modo texto. Esta herramienta se denomina Midnight Commander y se ejecuta con la orden:

$ mc

Podemos combinar varias instrucciones en la shell por medio de **redirecciones, tuberías y filtros**.

- **Redirecciones:** Con el carácter < puedo redirigir la entrada de datos de un proceso desde un archivo, sustituyendo así al teclado del terminal.

  $ cat </etc/passwd - El comando cat recibe como entrada el fichero /etc/passwd

  Con el carácter > redirijo la salida de un proceso a un archivo en lugar de la pantalla del terminal. Si existiese el archivo, quedará eliminado. Ejemplo:

  $ echo hola > saludo.txt - Escribirá hola en el archivo saludo.txt

  El operador de redirección >> también redirige la salida pero, si el archivo existe, la información se anexa.

- **Tuberías (pipeline):** Las tuberías permiten enlazar las salidas de unos programas con las entradas del siguiente.

  cat alumnos.txt | *more* - Muestra el contenido del archivo de página en página

- **Filtros:** Cualquier programa que lea de su entrada estándar y escriba en su salida estándar se denomina filtro. Los filtros permiten realizan tareas más sofisticadas sobre la entrada como: ordenación de la entrada; selección , búsqueda y sustitución de patrones, etc. pudiendo alcanzarse un grado considerable de complejidad cuando se concatenan entre sí. A continuación se estudian algunos de los filtros más básicos como son wc, sort, cut, grep, more y less:

  - wc [-lwc][archivo1 ...]: wc cuenta el número de caracteres, palabras y líneas por cada archivo que recibe como parámetro y el total de cada una de las categorías para todos los archivos.
    - -c cuenta únicamente el número de caracteres.
    - -l sólo el número de líneas.
    - -w sólo el número de palabras.
  - cat texto.txt | wc -l: cuenta el número de líneas en el archivo texto.txt
  - sort [dfn] [archivo1 ...]: Ordena las líneas de los archivos y las envía a la salida estándar
    - -d sólo las letras, dígitos y blancos son significativos en ordenación
    - -f ordena sin distinguir las mayúsculas de las minúsculas.
    - -n interpreta los valores a ordenar como numéricos.
  - cat alumnos.txt | sort >alumnos_ordenados.txt: Visualiza el fichero alumnos_ordenados.txt
  - grep 'caracteres' arch1 arch2 ...: Busca por fichero, mostrando aquellas líneas que contienen el conjunto de caracteres buscado
  - cat archivo | grep sh: Muestra las líneas que contienen sh
  - more archivo: Muestra el contenido del archivo pantalla a pantalla, se sale con q
  - less archivo: Igual que more pero podemos movernos con los cursores

Si estamos trabajando en un entorno como la shell, donde se manejan comandos para dar órdenes al sistema operativo de lo que queremos realizar, es posible que necesitemos almacenar algunos datos que nos permitan simplificar algunas labores repetitivas.

- **Alias:** Cuando usamos mucho un comando con una serie de parámetros y opciones, es posible definir un alias que realice lo mismo pero que sea más fácil de recordar y escribir.

  alias ll='ls -lrt -color=auto'

- **Rutas o camino (path)**: Cuando utilizamos un archivo o un comando éste debe estar en el directorio de trabajo en que nos encontremos, si no ocurre esto, debemos indicar la ruta o camino que debe seguir el intérprete de comandos para encontrar el archivo o el comando. Podemos indicar dicha ruta de forma directa o completa o con ruta relativa.

Cuando usamos la **Shell**, podemos definir el valor de variables que personalizan nuestro entorno o que son útiles para el funcionamiento de nuestros programas. Algunas son:

- PATH: Contiene el conjunto de caminos empleados para buscar las ordenes a ejecutar. Se pueden especificar múltiples caminos separándolos mediante el signo ":" (dos puntos).

Mediante la orden **'unset'**, las variables de entorno pueden ser eliminadas.

El sistema

Multiproceso. Indica que en un instante de tiempo determinado puede haber varios programas cargados en memoria compitiendo por el uso de la CPU. En los sistemas **monoprocesador**, los distintos procesos deben repartirse el tiempo de CPU. Este reparto lo lleva a cabo el **planificador** (**scheduler**). En los sistemas **multiprocesador**, puede haber varios procesos ejecutándose en paralelo. Un **proceso** es un programa cuando se encuentra en ejecución. Un proceso puede estar en diferentes estados: en ejecución, preparado o en espera.

Cuando arranca el sistema se inicia la ejecución de una serie de procesos. Primero se carga el núcleo de Linux (Kernel) de una forma totalmente especial y distinta a otros procesos. Seguirá un proceso llamado **'init'**, que es un proceso que va a generar nuevos procesos según el archivo initab.

Los permisos de los archivos se almacenan en **binario** aunque se pueden referenciar en decimal. A cada permiso le asociamos un número de tres dígitos formado por dos ceros y un tercer número que podía ser únicamente 1, 2, ó 4. Algunos comandos son:

- chmod [ugoa] =+- rwxst archivo
  chmod [ugoa] =+- rwx directorio
  Cambia el modo o permiso, para el usuario (u), grupo (g), otros usuarios (o) o para todos (a). Por defecto usa **a.** El carácter + da permiso, - lo quita, = lo fija. **r** lectura, **w** escritura, **x** ejecución, **s** el usuario adquiere la personalidad del propietario, **t** archivo rápido alojado en swap
- chown usuario arch1 arch2
  Se emplea para cambiar de propietario ("change owner") a un determinado conjunto de archivos. Este comando sólo lo puede emplear el actual propietario de los mismos.
- chgrp grupo arch1 arch2
  Cambia el grupo al que pertenecen los archivos.
- groups usuario: Da información del grupo
- id usuario: Da información del usuario

Un proceso puede iniciar a otro proceso (hijo). Además, existe la posibilidad de que dentro de un proceso existan varios **hilos de ejecución**, que serán módulos ejecutándose al mismo tiempo, compartiendo algunos recursos, como la memoria de datos. Esto permite transiciones entre programas muy rápidas.

Cuando se ejecuta un programa, éste no le devuelve el control al usuario hasta que no termina su ejecución, de manera que no es posible que un usuario pueda ejecutar varios programas simultáneamente. Como solución la **Shell** propone la ejecución de tareas en segundo plano o background. Esto se hace poniendo al final el carácter &

Todos los procesos están identificados por el sistema operativo con un número identificador de proceso (**PID**). Además tendrá su dueño, que será el proceso que lo inició o el usuario que lo ejecutó. También tendrá un número de prioridad que le indica al planificador cómo debe atender sus demandas. Algunos comandos son:

- ps: Muestra una lista de los procesos en ejecución
- ps u: Muestra los procesos que pertenecen al usuario actual
- ps aux: Muestra información detallada de los procesos en ejecución
- top: Muestra información del sistema: usuarios, hora, información del tiempo de funcionamiento de la máquina, número de procesos, uso de CPU, uso de memoria, y uso del swap. Además, incluye una lista de procesos similar a ps con la diferencia de que ésta se actualiza periódicamente, permitiéndonos ver su evolución.
- pstree: Muestra las tareas y sus subtareas en una estructura anidada
- kill [señal] PID: Se usa para enviar señales a los procesos
- kill -9 1283: Finaliza de forma inmediata la ejecución del proceso con PID 1283
- nice -n prioridad orden: Inicia el proceso con una determinada prioridad, -20 alta, 20 baja.
- renice prioridad PID: Modifica la prioridad del proceso PID
- shutdown: Es un comando para cerrar el sistema
- shutdowm -h now: Finaliza el sistema, equivale a halt
- shutdowm -r now: Reinicia el sistema, equivale a reboot.
- uname -a: Conseguimos toda la información del sistema

En los sistemas Linux **todo son ficheros**, es decir, cualquier elemento presente en el sistema es tratado como un archivo desde nuestros documentos personales hasta los dispositivos hardware como la impresora, el ratón, los discos duros, etc. Estos ficheros están organizados en lo que se conoce como un **Sistema de ficheros.**

Los discos de almacenamiento deben prepararse para su uso por el sistema operativo, es lo que se denomina "formatear", que comprende dos procesos:

- el formateo de bajo nivel
- la creación del sistema de ficheros.

En este proceso se escriben unas marcas en el disco para distinguir las pistas y sectores, que posteriormente pueden ser accesibles para la localización de archivos. Sobre ese disco formateado se pueden establecer particiones, que serán divisiones lógicas del disco.

Linux soporta, además de los tipos de sistemas de ficheros nativos (Minix, Ext, Xia, Ext2 y Ext3), varios sistemas de ficheros ajenos para facilitar el intercambio de datos con otros sistemas operativos. Algunos de los sistemas de ficheros soportados por Linux son:

- **ext2** Sistema de archivos estándar de Linux.
- **ext3** Sistema de ficheros que mejora al anterior y que usa esta versión de Guadalinex. Tiene la ventaja de que es de tipo *journaling* (se reduce el tiempo de recuperación tras un apagado inesperado).
- **msdos** Permite la compatibilidad con el sistema de ficheros FAT del MS-DOS.

- **vfat** Permite la compatibilidad con sistemas Windows 9x (Fat32).
- **ntfs** Acrónimo de *new technology file system*, y permite la compatibilidad con el sistema de ficheros de Windows 2000/XP.
- **iso9660** Es el tipo de sistema de ficheros estándar para CDROM.
- **umsdos** Extiende el sistema de ficheros msdos bajo Linux, de forma que desde Linux se pueden usar nombres de fichero largos, propiedad, permisos, enlaces y ficheros de dispositivo.
- **hpfs** Permite la compatibilidad con el sistema de ficheros de OS/2.
- **nfs** Es un sistema de ficheros de red que permite compartir sistemas de ficheros entre varios ordenadores.
- **sysv** Permite la compatibilidad con UNIX SystemV/386, Coherent y Xenix.
- **minix** Primer sistema de ficheros utilizado para Linux
- **ext** Primer sucesor de minix en desuso.
- **xiafs** Sucesor del ext en desuso
- **proc** Sistema de archivos virtual de Linux.

Existe además, generalmente, una partición o sección en el disco usada por el gestor de memoria conocida como área de **swap** (intercambio). A través ella el gestor de memoria implementa la memoria virtual. Los sistemas de ficheros se crean con el comando mkfs (Make Filesystem). La sintaxis de este comando es:

- mkfs [-t sistfich] dispositivo: Sistfich es el argumento mediante el que se pasa el tipo de sistema de ficheros a crear (ext3, ext2, hfs, etc)
  dispositivo o partición del disco donde crear el sistema de ficheros (/dev/hda1, /dev/sda3, /dev/fd0, etc), o también podría pasársele el punto de montaje (/tmp, /users, etc).
- mkfs -t vfat /dev/fd0: Crea un sistema de ficheros de tipo vfat en un disquete

Montar significa crear un acceso en el sistema de archivos. Todos los dispositivos están representados por un archivo del directorio /dev, por ejemplo en el caso de un disquete será seguramente /dev/fd0

- mount -t tipo dispositivo montaje: Monta el dispositivo con el sistema de archivos indicado en el tipo en el punto de montaje especificado.

Cuando finalicemos el uso de la unidad debemos **desmontarla** para evitar la pérdida de información. El comando es:

- umount /mnt/floppy: Desmonta la unidad, no debemos sacar el disco si no hemos desmontado la unidad

Si ocurriese un apagado indebido del ordenador sin haber cerrado el sistema y Linux solicitase una recuperación manual del sistema de ficheros, entonces deberá ejecutar el siguiente comando desde una terminal:

- /sbin/fsck/ /dev/hda1: Para arreglar la primera partición primaria del primer disco duro, suponiendo que contenga a Guadalinex.
- /sbin/fsck -a /dev/hda2: Realiza el proceso sobre la segunda partición del disco y evita las preguntas en el proceso (-a)

Scripts

Un **Shell Script** o programa **Shell** es un archivo que contiene un conjunto de órdenes que pueden ser interpretadas y ejecutadas por el **Shell**. Para que el **Shell** pueda ejecutarlo hay que activar los permisos de ejecución adecuados.

En la primera línea se pone: #!/bin/bash que indica que se trata de un script y le dice a la **Shell** donde se encuentra el intérprete de comandos.

Los programas Shell pueden recibir argumentos por la línea de comandos, están asociados a los nombres de variable siguientes:

- $0: identifica al nombre del programa,
- $1: identifica al primer argumento pasado al programa por la línea de órdenes,
- $2: identifica al segundo argumento de la línea de órdenes, y así sucesivamente

Configuración de la red

El interfaz de red para una red Ethernet será:

- eth0, para un módem será ppp0.
- o para el caso del interfaz de bucle cerrado loopback lo.

Para conectar nuestro ordenador a una red deberemos conocer ciertos datos de la red, concretamente: Dirección IP de nuestro sistema, máscara de la red, dirección IP del router de salida y dirección de los servidores **DNS**. Si en la red hay un servidor de **DHCP**, solamente tendremos que decirle a nuestra máquina que tome la configuración de red de forma dinámica mediante este protocolo y estos valores se asignarán automáticamente.

El comando ifconfig se usa para dar acceso al **kernel** a una interfaz física. El comando route permite añadir o quitar rutas de la tabla de encaminamiento del kernel. Por ejemplo:

```
# ifconfig eth0 176.10.0.10 netmask 255.255.255.0
```

Esto asigna a la interfaz eth0 la dirección IP 176.10.0.10 con la máscara de red 255.255.255.0. Podemos ver el resultado con la orden:

```
# route add -net 127.0.0.0 netmask 255.0.0.0 lo
# route add -net 176.10.0.0 netmask 255.255.255.0 eth0
```

Estamos indicando que en nuestra máquina, a la red 176.10.0.0, se llega a través de la interfaz eth0. Y a la red 127.0.0.0 llegamos a través del interfaz lo. La opción add del comando route añade rutas, con la opción del las eliminamos y con la opción -n las muestra.

Configuración de la impresora

Para instalar una impresora lo primero es comprobar si el demonio de impresión "cuspd" está a la escucha. Algunos comandos son:

- lp -d cola archivo: Imprime en la cola de impresión indicada el archivo
- lp hola.txt: Imprime el archivo hola.txt en la impresora por defecto

- lp -d fotos imagen.jpg: Imprime en la cola fotos el archivo jpeg
- lpstat -p -d: Muestra las colas de impresión disponibles y la predeterminada
- lpadmin -d impresora: Fija la cola de impresión predeterminada
- lpadmin -d borrador: Fija la cola predeterminada a borrador

Configuración del servidor X

Xwindow permite utilizar un ambiente gráfico bajo Linux, a diferencia de la terminal que es en modo texto. Utiliza una metodología cliente-servidor, esto es, existe un servidor X que es el encargado de generar y procesar gráficas, requisiciones, seguridad, etc; y un cliente X que solicita y recibe todas las requisiciones del servidor X.

Una vez que haya instalado todas las librerías y paquetes relacionados con **X** se puede configurar la instalación del **Servidor X** , la herramienta más común es Xconfigurator, que genera el archivo de configuración XF86Config ubicado en el directorio /usr/X11R6/lib/X11 (XF86 es el **servidor X** que es distribuido con Linux). Contiene el tipo de tarjeta de vídeo, resolución de monitor, tipo de ratón y otras configuraciones de su ambiente gráfico; el archivo XF86Config contiene los valores que serán utilizados por el **servidor X** , sus detalles de configuración son muy extensos.

Aplicaciones cliente, FTP, Telnet...

- El protocolo **telnet** es una herramienta muy útil a la hora de administrar sistemas basados en Linux. Permite acceder a una máquina remotamente de la misma forma que lo haríamos si estuviéramos sentados delante de la consola y utilizásemos su teclado para introducir los comandos. Nos proporcionará un mecanismo para conectarnos a un servidor remoto y ejecutar comandos en él de forma totalmente interactiva. El punto débil de este protocolo es que todos los datos se transmitirán en texto plano por la red.

- El servicio **ftp** se utiliza para cargar y descargar archivos de la red. Este servicio puede verse dividido en dos partes: Los usuarios con cuenta en el sistema pueden acceder a su propio sistema de archivos y cargar y descargar información y utilización anónima, en la que se permite que cualquiera se conecte.

- El protocolo **ssh** (**Secure Shell***)* permite realizar conexiones remotas seguras ya que la información no viaja en texto plano sino codificada. **ssh** cifra los datos antes de pasarlos a la red, descifrándolos cuando llegan a su destino. El procedimiento de cifrado asegura que el intruso que capture los datos será incapaz de descifrarlos y verlos.

- Podemos realizar estas operaciones de telnet y ssh desde el entorno gráfico usando el programa: gnome-remote-shell. Sólo hemos de escribir el nombre o IP de la máquina con la que vamos a iniciar la conexión, el tipo de protocolo a usar (telnet o ssh)

10. Linux (III): Administración y configuración

Administración

La persona que se dedica a mantener funcionando un sistema informáticose llama administrador del sistema y sus funciones más importantes son:

- Gestionar a los usuarios, sus derechos y permisos sobre los recursos.
- Ser capaz de reparar el sistema ante una caída, fallo hardware o malfuncionamiento en general. Incluyendo la realización y posible restauración de copias de seguridad.
- Actualizar el software instalado con nuevas versiones e instalar nuevas aplicaciones
- Instalar y configurar nuevos elementos hardware (discos, impresoras, tarjetas de red...)
- Implantar medidas de seguridad que garanticen a los usuarios del sistema la protección necesaria ante amenazas internas (red local) o externas (Internet).

Las herramientas con las que cuenta el administrador son extremadamente simples:

- Terminal de comandos del sistema, *shell*.
- Editor de texto plano
- Documentación del sistema. Las más accesibles son las páginas del manual en pantalla *man*,

Toda la **configuración de un sistema Linux** se administra editando unos **archivos** que normalmente están en el directorio **/etc**. Son de texto plano. Cada uno de esos archivos guarda la configuración de una parte del sistema, de una aplicación concreta o de la forma de comportarse el sistema ante una situación dada.

Editar los ficheros de configuración directamente puede ser una **labor complicada y peligrosa**, ya que si no se hace bien **podemos desconfigurar el sistema** o hacer que se vuelva inestable. Siempre será **preferible** hacerlo a través de **menús gráficos** como el presentado en el apartado anterior o utilizando un **comando de *shell*** que realice la tarea de una forma ordenada y segura. No todo se puede hacer con interface gráfico, pero todo se puede hacer con comandos. La conclusión es que un buen administrador de sistema debe estar acostumbrado a usar una terminal de entrada de órdenes, la más utilizada en Linux es bash.

Los **scripts** son archivos de texto que contienen la secuencia de comandos para realizar un tarea concreta. Son muy importantes en la administración del sistema para automatizar tareas en el arranque y parada del sistema operativo. Un script es como un programa confeccionado con comandos, instrucciones de control y variables. En /etc/init.d existen multitud de scripts de sistema, la mayoría sirven para arrancar o parar servicios del propio sistema operativo.

Gestión de usuarios y grupos de usuarios

Linux utiliza dos ficheros de configuración para gestionar a los usuarios, los dos están en **/etc** y se llaman **passwd** y **shadow**.

- **Archivo *passwd***: Contiene la **lista de usuarios del sistema**, incluidos *root* y los usuarios especiales asociados a los servicios. De cada usuario se guarda su nombre, identificador numérico, identificador de grupo, ruta al directorio de trabajo (HOME) y shell utilizada (por defecto bash). Este archivo es propiedad de root pero cualquier usuario del sistema tiene

derecho de lectura sobre él.

- **Archivo shadow:** Contiene la lista de usuarios del sistema junto con su contraseña encriptada, este archivo es propiedad de root y sólo él puede leerlo. En esto se basa la seguridad de todo sistema linux.

Para **gestionar los grupos** se utiliza el **archivo *./etc/group*** que mantiene la **lista de grupos** y los usuarios de cada grupo.

Sólo root y aquellos usuarios que hayan sido autorizados por él pueden crear usuarios en el sistema. En el proceso de creación de un usuario se producen los siguientes hechos.

- Se crea un nuevo subdirectorio en el directorio /home con el nombre del nuevo usuario.
- Se crea una entrada en el archivo /etc/passwd con el nombre de usuario, su directorio de trabajo, su shell, sus identificadores numéricos de usuario y grupo y opcionalmente su nombre completo, dirección teléfono, etc.
- Se crea una entrada en el archivo /etc/shadow con el nombre de usuario, su contraseña encriptada y una serie de campos que indican informaciones tales como la duración de la contraseña, el número de días desde el último cambio,...
- Se crean entradas en el archivo /etc/group para indicar a qué grupos pertenecerá el nuevo usuario.
- Se configura por defecto el entorno de trabajo del nuevo usuario. Esto se consigue con archivos ocultos dentro de su directorio HOME que expresan la configuración del escritorio y de las aplicaciones instaladas, por ejemplo los favoritos del navegador web mozilla se guardan en .mozilla.

Lo podemos hacer de dos maneras.

- Utilizando el comando useradd: En su forma más simple sería useradd nuevo_usuario.
- Utilizando la aplicación gráfica incluida en GNOME:

El comando

$ passwd nombre_de_usuario

cambia la contraseña de un usuario. Las ódenes para el mantenimiento de usuario son:

- Borrar un usuario
  $ userdel userdel [-r] login

- Modificar usuario
  $ usermod usermod [-d home [-m]] [-G grupo] [-l login] [-p password] usuario

- Añadir un grupo
  $ groupadd groupadd grupo

- Borrar un grupo
  $ groupdel groupdel grupo

- Modificar un grupo
  $ groupmod groupmod [-n nuev_nombre] grupo

Conocer el sistema

Algunos comandos importatnes son:

- **users**: nos muestra la lista de usuarios conectados en un momento dado
- **who**: nos muestra la misma información y además permite conocer, por ejemplo, el tiempo de inactividad de cada usuario. -u: Tiempo de inactividad -H: Imprime cabeceras en las columnas
- **whoami**: te dirá cual es el usuario conectado
- **hostname**: Saber el nombre del sistema y cambiarlo
- **kernelversion**: Saber la versión del kernel
- **dmesg**: Saber el hardware sobre el que se está ejecutando
- **uname**: Información completa del sistema. uname [-a] Toda la información disponible
- **df**: Informe de utilización del espacio en disco de cada partición. -k: Expresado en kbytes -m: Expresado en megabytes
- **mount**: Lista de particiones montadas, sistema de ficheros, etc.
- **free**: Ver estado de la memoria. -m: Cantidades expresadas en megabytes
- **ifconfig**: Conocer el estado y configuración de los interfaces de red. ifconfig [interface]
- **route**: Conocer la tabla de enrutamiento actual

Linux tiene disponibles para el administrador varios comandos que permiten monitorizar el estado de los procesos e incluso detenerlos o "matarlos" si han quedado bloqueados. También existen las correspondientes herramientas gráficas para el escritorio GNOME. Cada proceso tiene un número asignado y también tiene un proceso padre que es el que lo ha creado,

- cuando ejecutamos un programa se lanzan uno o varios procesos
- y cuando el programa termina los procesos desaparecen liberando los recursos (CPU y memoria) que tenían asignados.

Algunos comenados son:

- **ps:** Listar los procesos que existen en el sistema. -u: Lista sólo los procesos de ese usuario -x: Lista los procesos que no están asignados a una terminal
- **top**: Monitorizar los procesos y sus características en formato carácter

Arranque y parada de sistema. Niveles de ejecución. Demonios

Dos de los momentos más delicados en la operación del sistema operativo y donde más cosas ocurren es en el arranque y parada del mismo. Las secuencias de arranque y parada deben producirse en un orden concreto porque cada paso depende de los anteriores. Un administrador de sistema debe conocer a fondo lo que pasa en estas situaciones

Durante el arranque:

- El programa de arranque del ordenador que está en memoria ROM inicializa varios aspectos del hardware. Después, de acuerdo a su configuración, carga el primer sector de un disquete o de un disco duro o de un CD-ROM y ejecuta el programa que allí se encuentra.
- Si disponemos de varios sistemas operativos instalados en nuestro ordenador podremos escoger cuál cargar por medio de un gestor de arranque (como LILO o GRUB). Si escogemos arrancar el sistema operativo Linux el gestor de arranque cargará el kernel en memoria y lo descomprimirá (se encuentra comprimido en disco para que ocupe menos

espacio).

- El kernel:
    - detecta algunos detalles del hardware (como el procesador, cantidad de memoria y algunos dispositivos),
    - procesa parámetros recibidos del cargador de arranque,
    - inicializa algunos aspectos del hardware,
    - prepara áreas de memoria,
    - prepara el sistema de archivos virtual o swap y lanza como primer proceso **/sbin/INIT**. Éste es un proceso padre de todos los demás. Varios de los mensajes que el kernel produce durante esta etapa pueden ser revisados en el archivo /var/log/dmesg y con el programa dmesg.
      Como los dispositivos de cada ordenador son diferentes, el kernel cuenta con controladores para muchos tipos de hardware diferentes y para no ocupar tanto espacio en memoria el kernel emplea un sistema de módulos. Si todos los controladores para todos los tipos de hardware que el kernel soporta, se incluyeran directamente en el kernel desde el arranque, el kernel requeriría mucha memoria RAM. Por eso se pueden incluir o quitar controladores por medio de módulos cargables. Se dice que el kernel de Linux es modular. Un **módulo** es una parte del kernel que puede cargarse, usarse o quitarse después de que el kernel está funcionando.
        - Algunos módulos ofrecen servicios (por ejemplo soporte para ciertos sistemas de archivos)
        - y otros son controladores para hardware específico (por ejemplo hay módulos para tarjetas de sonido, para tarjetas de red, etc.).
    - Durante el proceso de inicialización del sistema, algunos dispositivos son detectados y se cargan los módulos apropiados.
- El programa /sbin/init, que normalmente es el primer proceso ejecutado por el kernel completa la secuencia de inicialización ejecutando los procesos del nivel de ejecución fijado en el archivo /etc/inittab.
- A continuación se inician las terminales en modo texto (por defecto en Guadalinex de la 1 a la 6) que permiten a los usuarios iniciar sesiones tipo texto con el intérprete de comandos.
- Por último, si se ha configurado el sistema para arrancar el sistema de gráficos, se lanza el servidor X-Windows y sobre él, el escritorio elegido, GNOME o KDE.

Nivel de ejecución

Un **servicio** se traduce en la práctica en la ejecución de uno o más procesos que están cargados en memoria a la espera que algún otro proceso solicite su ejecución, a estos procesos-servicio se le denomina demonios (daemons). En el arranque se activan muchos de estos servicios de forma automática, pero para hacer el sistema más flexible se pueden establecer distintas configuraciones de servicios activos, esto es lo que se conoce como **niveles de ejecución.** Cada nivel de ejecución está destinado a configurar al sistema para una modo concreto. Podemos pasar de un nivel de ejecución a otro parando los servicios disponibles en un nivel y arrancando los servicios del otro. El nivel de ejecución por defecto en el arranque se define en el archivo de configuración /etc/inittab. Los distintos niveles de ejecución son:

- 0 Parada
- 1 Monousuario
- 2 Multiusuario en modo texto
- 3 Multiusuario en modo texto con funciones de red
- 4 No utilizado
- 5 Multiusuario en modo gráfico
- 6 Reinicio

Para implementar los niveles de ejecución se utiliza el ya mencionado /etc/inittab y el directorio /etc/init.d. En este último existen scripts de arranque/parada de cada uno de los servicios instalados. Todos los scripts de /etc/init.d se pueden llamar con los parámetros start, stop y restart,

Por otra parte en /etc existen 6 directorios llamados rc0.d, rc1.d, rc2.d, rc3.d, rc4.d, rc5.d y rc6.d. En ellos existen unos archivos especiales cuyos nombres empiezan por "S" o "K" y que son los encargados de arrancar ("S") los servicios de un nivel o parar ("K") servicios para ese nivel.

Algunos comandos importantes son (sólo root):

- init [número de nivel]: Cambiar de nivel de ejecución
- runlevel: Ver el nivel de ejecución actual
- shutdown -h now: Parar el sistema (halt). De forma inmediata
- shutdown -t now: Reiniciar el sistema (reboot). De forma inmediata.

Parar un sistema Linux es lo mismo que llevarlo al nivel de ejecución 0 (halt). Puede ser con: “shutdown -h now” o “init 0”. La parada de un sistema es más simple que el arranque y básicamente consiste en:

- Parar de forma ordenada todos los servicios que estuvieran activos
- Desconectar a los usuarios activos (si hubiera alguno)
- Desmontar de forma correcta los sistemas de ficheros montados en ese momento.

Instalación y actualización de aplicaciones

Hay que tener en cuenta que algunas aplicaciones requieren para su instalación que otras aplicaciones o librerías estén instaladas previamente, a esto se le llama **dependencias**. Las aplicaciones en Linux se pueden instalar de dos formas:

- Instalación desde el código fuente: Esta forma es la más general porque puede ser usada sin importar la distribución de Linux que estemos utilizando, pero también suele ser la más incómoda.
- Instalación desde paquetes precompilados: Este método es mucho más cómodo y nos asegura que la aplicación se instalará en la forma correcta sin necesidad de compilar los códigos fuentes.

En las distribuciones basadas en Debian existe un archivo para configurar los sitios de Internet desde los que nuestro sistema descargará los paquetes de instalación, este archivo es /etc/apt/sources.list. Existen varias aplicaciones para la instalación de paquetes:

- La aplicación **apt** consta de varios programas independientes en modo comando para actualizar e instalar aplicaciones a partir de paquetes en formato deb descargadas de las fuentes indicadas en el archivo /etc/apt/sources.list. Los comandos son:
    - apt-get update: Actualiza los paquetes disponibles a partir de los repositorios
    - apt-get upgrade paquete: Actualiza a la última versión disponible en los repositorios el paquete previamente instalado en el sistema.
    - apt-get install paquete: Instala un paquete que está en los repositorios
    - apt-get remove paquete: Desinstalar un paquete y sus dependencias
- La aplicación **Synaptic** realiza las mismas funciones que apt, pero está integrada en el escritorio GNOME y tiene apariencia gráfica

Administración de los sistemas de ficheros

En la siguiente tabla se muestran los sistemas de ficheros más importantes que son soportados por Linux.

- ext3 El habitual sistema de ficheros de los sistemas Linux actuales.
- ext2 Antecesor de ext3.
- iso9660 Sistema de ficheros utilizado por unidades de CD ROM.
- minix Sistema de ficheros utilizado originariamente en Minix.
- msdos Sistema de ficheros utilizado por algunos sistemas operativos de Microsoft.
- swap Sistema de ficheros utilizado para las particiones de intercambio. Éstas se utilizan para almacenar datos temporalmente cuando la RAM está llena.
- nfs Sistema de ficheros en red utilizado por Linux.
- vfat Sistema de ficheros para sistemas Windows de Microsoft.

Existe un archivo donde se guarda la configuración de los sistemas de ficheros que se pueden montar en nuestro sistema Linux. Este fichero es */etc/fstab* y es propiedad de *root*, por lo tanto sólo el administrador puede hacer cambios en él. La estructura del fichero *fstab* es sencilla, una línea por cada sistema de ficheros y 6 campos por cada línea. A continuación se especifica el contenido de cada campo:

- Nombre de dispositivo: Es el nombre de dispositivo físico. Suele ser un dispositivo de los incluidos en el directorio /dev.
- Punto de montaje: Es el directorio donde se montará el sistema de ficheros.
- Tipo de sistema de ficheros
- Opciones de montaje: Las particularidades del montaje del sistema de ficheros, van separadas por comas. Las más importantes son:
    - *noauto*: Impide que se monte automáticamente en el arranque.
    - user: Se permite a cualquier usuario el montaje y desmontaje.
    - *ro*: Montaje en sólo lectura.
    - rw: Montaje en lectura/escritura.
    - noexec: No permite la ejecución de binarios en el sistema de ficheros montado. Útil para sistemas que no son Linux, como por ejemplo Windows.
    - *exec*: Permite la ejecución de binarios.
    - *defaults*: Emplea las opciones predeterminadas para este sistema de ficheros.
- Indicador de volcado: Tiene relación con el volcado de copias de seguridad, indicando si el sistema de ficheros será volcado o no.
- Indicador de comprobación: Indica si el sistema de ficheros será comprobado con el comando *fsck*.

Un ejemplo:

/dev/hda3 /mnt/w98 vfat ro,auto 0 0

Algunos comandos son:

- mount [punto_de_montaje]: Busca la línea de fstab donde se indican las opciones de montaje, tipo de sistema de ficheros y dispositivo que corresponden al punto de montaje.
- umount [punto_de_montaje]: Desmonta el sistema de ficheros que estaba montado en el punto de montaje.
- mount: Listar los sistemas de ficheros montados en la actualidad

Linux es especialmente válido en la interconexión de sistemas y uso en red, por eso merece especial mención el sistema de ficheros en red **NFS (Network File System)**. Es un tipo de

sistema de ficheros que sirve para montar sistemas remotos en el propio ordenador de forma que se pueden compartir datos en una red de ordenadores. NFS funciona en modo cliente servidor, de forma que un ordenador (servidor) pondrá alguno de sus directorios a disposición de los demás ordenadores (clientes) a través de la red (local o incluso Internet).

Para usar NFS podemos aplicar lo visto anteriormente para otros tipos de sistemas de ficheros con dos añadidos que dan la dimensión de red.

- En el servidor debemos especificar qué directorio o directorios se van a compartir y de qué forma (lectura, escritura, usuarios autorizados,...). Esto se hace por medio del archivo */etc/exports*.
- En los clientes se especifican los sistemas NFS que se pueden montar indicándolo en el archivo *fstab*. Habrá que especificar en qué ordenador de la red está el sistema a montar.

Un ejemplo. Supongamos que en el ordenador de la red llamado *servernfs* queremos compartir con los demás el directorio */publico* en acceso de sólo lectura (*read only*, *ro*). Para conseguir esto tendremos que configurar el archivo */etc/exports* del servidor (*severnfs*) y configurar los archivos */etc/fstab* de los ordenadores de la red indicando el punto de montaje en el cliente.

- etc/exports del ordenador servernfs /etc/fstab de los ordenadores clientes de la red
- /publico (ro) servernfs:/publico /mnt/pub nfs 0 0

Esto monta el directorio /publico del ordenador servernfs en el directorio /mnt/pub de los clientes para operaciones de lectura. Cuando desde un cliente se acceda a /mnt/pub en realidad se estará utilizando la información contenida en /publico del ordenador servernfs. También se puede especificar la dirección IP del ordenador servidor en lugar de su nombre.

Instalación y configuración de servicios de red en un servidor Linux

Algunos de los servicios de red que se pueden instalar y manejar en un sistema Linux son:

- **NFS**: El ya conocido sistema de ficheros en red.
- **DNS**: Servicio de resolución de nombres.
- **Servidor web:** Convierte a un sistema Linux en un servidor de páginas web.
- **Servidor FTP**: Permite transferir archivos utilizando el protocolo FTP.
- **Servidor Samba**: Es útil para integrar sistemas Linux en redes de ordenadores Windows.
- **Servidores POP3/SMTP**: Con estos se puede convertir un sistema Linux en un servidor de correo electrónico.
- **Servidor de base de datos**: El sistema puede servir datos almacenados en un sistema gestor de base de datos al resto de equipos de la red. Los gestores más utilizados son *MySQL* y *PostgreSQL*.
- **Servidor Proxy:** Uno de los usos más interesantes en una red local que puede ofrecer un sistema Linux. La aplicación más extendida es *Squid*.
- **Servidor de DHCP**: Convierte nuestro sistema Linux en un servidor de direcciones IP para los clientes de nuestra red.

11. Introducción a los sistemas operativos Microsoft. Windows XP instalación y operaciones básicas

El comienzo

Microsoft comienza con el desarrollo de MS-DOS, el primer sistema operativo de esta empresa. Fue instalado por primera vez en 1981 en una computadora IBM. Este sistema operativo era monousuario, monotarea y presentaba las salidas por pantalla en forma de caracteres, lo que se conoce como "interfaz modo texto".

En 1985 Microsoft lanzó Windows 1.0, un sistema operativo que ampliaba las prestaciones de MS-DOS e incorporaba por primera vez una interfaz gráfica de usuario. Posteriormente Windows 2.0, que salió a la venta en 1987, mejoraba el rendimiento y ofrecía un nuevo aspecto visual. Tres años más tarde apareció una nueva versión, Windows 3.0, a la que siguieron Windows 3.1 y 3.11.

Microsoft desarrolló en 1993 un sistema operativo enfocado a necesidades empresariales, denominado Windows NT. A partir de ese momento, Microsoft se divide en dos líneas de desarrollo:

- sistemas operativos Windows enfocados a usuarios domésticos como son las versiones 95, 98 y ME
- sistemas operativos Windows NT que más tarde darían lugar a las familias Windows 2000 y 2003, con funciones adicionales enfocados al mundo empresarial.

La primera línea de desarrollo enfocada al usuario doméstico gozaba de un mejor soporte a juegos, controladores de periféricos, etc. Por el contrario presentaba una mayor inestabilidad del sistema (cuelgues del sistema) característica no deseada que presentaban Windows 95 y 98.

Todos los Sistemas Operativos, desde Windows 1.0 a Windows ME necesitaban tener MS DOS instalado, aunque desde la aparición de Windows 95, podía instalarse Windows sobre un disco duro vacío, ya que durante su propia instalación, se instalaba además una versión reducida de MS DOS. La arquitectura de Windows comenzó siendo de 16 bits, hasta Windows 95, donde pasó a funcionar bajo una arquitectura de 32 bits, aunque manteniendo bastantes módulos de 16 bits por razones de compatibilidad.

La segunda línea de desarrollo (NT) se basaba en emplear desde el origen un sistema operativo en modo gráfico y con una arquitectura de 32 bits. Este Sistema Operativo no requiere tener instalado ningún otro previamente. Incluye en todas sus versiones, un emulador de consola en modo texto.

Windows XP

Fue hecho público el 25 de octubre de 2001 por Microsoft. Microsoft inicialmente sacó a la venta dos versiones: Home (mercado doméstico) y Professional (entornos empresariales, como la autenticación por red y el soporte multiprocesador).

Windows XP es el intento por parte de Microsoft de ofrecer un único sistema operativo multiuso, con el inconveniente de eliminar definitivamente el soporte para los programas basados en MS-DOS del sistema operativo. Windows XP está basado en el código de Windows 2000 con un nuevo interfaz gráfico (llamado Luna), el cual incluye características ligeramente rediseñadas

En noviembre de 2002, Microsoft sacó a la venta dos nuevas versiones de Windows XP para hardware específico:

- Windows XP Media Center Edition para PCs especiales. Actualmente, dichos PCs son los "HP Media Center Computer" y la serie "Alienware Navigator". "Windows XP Media Center Edition"
- Windows XP Tablet PC Edition para ordenadores portátiles especiales diseñados con una pantalla táctil que admiten escritura a mano y pantallas tamaño portarretratos.

El 28 de marzo de 2003, Microsoft hizo pública otra versión: Windows XP 64 Bit Edition para fabricantes cuyo destino son los procesadores AMD 64 e Intel con extensiones de 64 bits.

Instalación de Windows XP

Primero se tienen que hacer copias de seguridad de los archivos importantes, luego se verán las características Hardware necesarias para la versión del sistema operativo que vamos a instalar. Será:

- Espacio disponible en el disco duro o partición elegida para la instalación y requerida. Es recomendable dividir el disco (en el caso de uno solo) en al menos dos particiones, una para el sistema operativo y otra para datos
- Con el arranque debes saber que:
    - El proceso de arranque se puede realizar mediante un disquete previamente creado como "Disquete de arranque".
    - Actualmente los ordenadores permiten arrancar directamente desde el CD-ROM. Para ello habrá que configurar previamente la BIOS si no lo está, para que inicie el proceso de arranque desde la unidad de CD-ROM antes que de disco duro
- Hay que indicar qué sistema de archivos queremos utilizar. Entre las que nos permitirá FAT o NTFS. Las características más destacables de cada uno de estos sistemas de archivos son:
    - FAT32
        - Admite particiones de hasta un máximo de 32 GB en Windows XP.
        - Tamaño máximo de archivo 4 GB.
        - Máximo número de clusters 65.536.
        - No permite trabajar con Dominios.
        - Se puede convertir a NTFS.
    - NTFS
        - Permite particiones de más de 2 Terabytes.
        - El tamaño de archivo máximo puede ser tan grande como la partición.
        - Sin límite de cluster, permitiendo un tamaño de cluster de 512 bytes.
        - No se puede convertir a FAT32.
        - Funciona mejor en grandes particiones.
        - Ofrece mayores posibilidades de seguridad. Permite trabajar con dominios.

12. Uso avanzado de Windows XP

Características y versiones Windows XP

Windows XP aparece como una síntesis de los sistemas Windows 9x y Windows 2000, de manera que mantiene la funcionalidad y adaptabilidad al usuario doméstico de los Windows 9x, con la seguridad y robustez de los sistemas Windows NT, 2000. Las características fundamentales que aporta Windows XP con respecto a las versiones anteriores:

- **Compatibilidad de las aplicaciones:** se pueden ejecutar aplicaciones antiguas compatibles con los sistemas operativos anteriores de Microsoft, ofreciendo además, un modo de compatibilidad (Asistente para Compatibilidad de programas) para aquellas aplicaciones que no se puedan ejecutar en el modo normal de funcionamiento de Windows XP. Además se incluye, el Soporte DLL colateral: permite utilizar distintas versiones de las librerías dll, lo cual permite una mayor compatibilidad con diferentes tipos de software.
- **Soporte para hardware y dispositivos:** se ha mejorado y ampliado la compatibilidad del sistema operativo con el hardware existente, sobre todo, para los periféricos conectados a USB (Universal Serial Bus) y al bus de alta velocidad IEEE 1394 o FireWire. Además, se incluyen el Comprobador y el Restaurador de controladores de dispositivos hardware que evitan problemas con los controladores.
- **Mejoras en la instalación, actualización y reparación de Windows:** incluye un sistema de actualización automática a través de Internet (Windows Update) que se adapta a las características de nuestro equipo para mantener nuestro equipo actualizado y protegido ante posibles errores de programación o fallos de seguridad.
- **Un nuevo sistema de copias de seguridad, recuperación y restauración:** permite mantener de forma dinámica y automática nuestras copias de seguridad con un modelo de restauración que incluye un gestor inteligente de versiones, un compresor y un antivirus. Además el sistema de recuperación de fallos y restauración de Windows a un estado seguro anterior evita tener que reinstalar el equipo cuando este deja de funcionar por un problema de configuración.

Microsoft ha desarrollado de momento 5 versiones de Windows XP:

- Home: para usuarios domésticos
- Profesional: para entornos profesionales
- Profesional 64-bit: para entornos profesionales que utilicen ordenadores con arquitecturas de procesador de 64 bits
- Media Center: adaptado al hogar, integra posibilidades multimedia como televisión, vídeo digital, música digital, álbumes fotográficos, etc.
- Tablet PC: para equipos portátiles con reconocimiento de escritura manual.

Fundamentalmente, las diferencias se refieren a las posibilidades de interconexión con redes de ordenadores y a cuestiones de seguridad. En Home sólo podremos usar una red doméstica de pocos equipos con una seguridad baja debido a que no se espera la necesidad de una mayor protección; y en la Profesional, podremos utilizar topologías de red más complejas con un nivel de seguridad acorde a las necesidades de este tipo de redes en la empresa.

El 30 de abril de 2005 Microsoft lanzó su primer sistema operativo de 64 bits, el **Windows XP Professional x64 Edition**.

- Está creado para trabajar de forma específica con procesadores x64. El término x64 se utiliza para describir la arquitectura de 64-bit desarrollada por Advanced Micro Devices (AMD) e Intel que mantiene la compatibilidad con los anteriores procesadores de la familia x86.
- Su mayor aplicación está en los creadores de contenido digital, creaciones 3D, juegos, diseño industrial, dinámicas de fluido computacional, visualización científica, etc.
- Windows XP Professional x64 Edition **ejecuta también aplicaciones de 32-bit** en el subsistema de Windows on Windows 64 (WOW64) ofreciendo compatibilidad con las aplicaciones existentes de 32-bit Windows además de activar las nuevas aplicaciones de 64-bit.
- Windows XP Professional x64 Edition admite hasta 32 gigabytes (GB) de memoria RAM y 16 terabytes de memoria virtual, lo que permite que las aplicaciones se ejecuten más rápidamente cuando trabajen con grandes conjuntos de datos.
- Las aplicaciones de 64 bits pueden ofrecer más datos por ciclo de reloj, con lo que se ejecutan más rápidamente y de forma más eficaz. Mejora el rendimiento en los cálculos en punto flotante.

Microsoft ha revisado Windows XP incluyendo el llamado **"Service Pack 2"** que incluye numerosas mejoras al sistema operativo y útiles herramientas. Estas mejoras son:

- **Nuevo cortafuegos (Firewall):** impide las conexiones entrantes no solicitadas mediante TCP/IP versión 4 (IPv4) y TCP/IP versión 6 (IPv6), evita que los puertos escuchen la red excepto cuando los esté utilizando una aplicación.
- **Nuevas Opciones de Internet:** opciones de descarga de archivos desde Internet (en la sección Misceláneo), con las cuales Internet Explorer verificará la fiabilidad de un archivo por su contenido, uso del bloqueador de ventanas emergentes (pop up)
- **Actualizaciones Automáticas:** Windows Update, buscará actualizaciones de seguridad, las bajará a su PC y las instalará, todo de manera automática y sin la intervención del usuario. Este proceso se podrá programar, automatizar o realizar manualmente.

Configuración

Desde el **Panel de control** podemos tener acceso al centro de comandos de Windows.

Propiedades del Sistema

Si accedemos al icono de sistema desde la vista clásica, o a Rendimiento y mantenimiento desde la vista por categorías, tendremos acceso a las **Propiedades del Sistema**.

- En la ventana **General**, la herramienta nos da datos acerca de la versión e sistema operativo que tenemos instalada, los datos de nuestro registro, y los datos de nuestro equipo.
- En la ventana del **nombre del equipo**, tendremos los datos de nuestro ordenador y del grupo y dominio al que pertenecemos.
- En "**hardware**" podremos conocer los controladores instalados, que deberán estar firmados si queremos asegurarnos una perfecta integración con el sistema y la ausencia de problemas de compatibilidad. El hardware instalado puede verse en el administrador de dispositivos y podemos tener diferentes perfiles de configuraciones hardware
- En **opciones avanzadas** disponemos de distintos menús para configurar nuestra máquina. En rendimiento, podemos optimizar la velocidad del equipo. Los perfiles de usuario permiten definir diferentes usuarios con sus características propias. Se pueden ver las variables de entorno y deshabilitar los informes de errores.
- En **restaurar sistema** permite configurar el sistema de restauración de Windows a un

estado seguro anterior.
- Las **actualizaciones automáticas** permiten tener Windows siempre actualizado para evitar fallos de seguridad o de programación.
- **Acceso remoto** nos faculta a configurar este sistema de asistencia remota.

Herramientas administrativas

Desde el panel de control podemos acceder a las **Herramientas administrativas** donde tendremos la opción de configurar y optimizar nuestro ordenador. Desde la herramienta **Administración de equipos** incluida accederemos a la mayor parte de las herramientas administrativas. Está organizado como una consola con forma de árbol denominada **Microsoft Management Console (MMC)**, tiene estructura jerárquica y permite ver fácilmente todos los elementos.

- **Herramientas del sistema**: incluye las que mostramos en el siguiente cuadro:
    - Visor de sucesos: podemos saber qué ha ido ocurriendo en nuestro ordenador y detectar posibles fallos
    - Carpetas compartidas: Muestra carpetas compartidas, sesiones actuales y archivos abiertos
    - Usuarios locales y grupos: Administra usuarios y grupos locales.
    - Registros y alertas de rendimiento
    - Administrador de dispositivos

- **Almacenamiento:** Muestra los dispositivos de almacenamiento instalados en el equipo que está administrando. Contiene: Almacenamiento extraíble, Desfragmentador de disco y Administración de discos

- **Servicios y aplicaciones:** contiene diversas herramientas predeterminadas que ayudan a administrar servicios como por ejemplo las conexiones Plug and Play.

Modos de arranque

Windows XP permite realizar un menú de arranque de manera que podamos disponer de diferentes sistemas operativos en nuestro ordenador, esta información se almacena en el archivo boot.ini. Además permite arrancar de diversos modos. Así se incluyen las opciones:

- **Modo seguro:** para arrancar en cualquier caso aunque con una limitación alta en la funcionalidad del sistema.
- **Modo de restauración:** para devolver el sistema a un estado anterior
- **Modo de depuración:** para realizar un seguimiento del arranque y localizar el problema.

Se puede habilitar el registro de inicio para crear un archivo NTBTLOG.TXT que contiene un listado con todo el proceso realizado durante el arranque.

Registro

El registro de Windows es una base de datos jerárquica que administra la información del sistema operativo necesita, fundamentalmente información relativa a la configuración del entorno, los perfiles de usuario, etc. La información del registro está alojada en los archivos:
- SYSTEM.DAT: incluye información del hardware del sistema
- USER.DAT: con información sobre los usuarios
- POLICY.POL: incluye las políticas de sistema para seguridad y administración de los recursos

El registro es editable mediante el programa REGEDIT.EXE. Las carpetas representan claves del Registro y se muestran en el área de exploración en el lado izquierdo de la ventana Editor del Registro. En el área de temas de la derecha, se muestran las entradas de una clave.

A continuación realizamos una descripción de las Carpetas o claves predefinidas:

- **HKEY_CLASSES_ROOT:** Aquí se almacena la información que asegura que se abre el programa correcto al abrir un archivo con el Explorador de Windows, además contiene datos de la configuración software de las aplicaciones instaladas en el ordenador.
- **HKEY_CURRENT_USER:** Contiene la raíz de la información de configuración del usuario que ha iniciado la sesión. Aquí se almacenan las carpetas de usuario, los colores de pantalla y la configuración del Panel de control. Se conoce como perfil de usuario.
- **HKEY_LOCAL_MACHINE:** Contiene información de configuración específica del equipo para cualquier usuario, incluye información sobre el hardware (tipo de bus, memoria, etc.) y el sistema operativo (controladores, configuración, etc.).
- **HKEY_USERS:** Contiene la raíz de todos los perfiles de usuario del equipo, incluye la configuración del escritorio, del entorno de Windows y la configuración personalizada del software
- **HKEY_CURRENT_CONFIG:** Contiene información acerca del perfil de hardware que utiliza el equipo local al iniciar el sistema, incluye datos acerca de los controladores de dispositivos que debe cargar.

Visor de suscesos

Es el encargado de monitorizar los sucesos del sistema, las aplicaciones y la seguridad de Windows. Se incluyen tres tipos de sucesos:

- **Registro de aplicación:** los sucesos sobre aplicaciones del sistema y su rendimiento.
- **Registro de sistema:** los inicios de componentes de Windows fallidos.
- **Registro de seguridad:** los sucesos de seguridad del sistema, inicios y cierres de sesión, los accesos a archivos y carpetas, etc.

Este visor crea categorías de los sucesos que a continuación comentamos:

- Sucesos de **información**: cuando el servicio o aplicación se ha cargado sin problemas.
- Sucesos de **aviso**: indican que algo podrá ir mal en el futuro
- Sucesos de **error**: avisan de que la aplicación o el servicio ha fallado al cargarse.

Actualizaciones del sistema operativo

La herramienta es Actualizaciones Automáticas en el Panel de Control. Podemos especificar cómo y cuándo deseamos que Windows actualice su equipo.

Configuración y uso de una red de ordenadores

Conexión de dos PC

Se hace desde **Panel de control**, y abrimos **Conexiones de red**. Seleccionamos **Crear conexión nueva**. Seguimos los pasos en los dos ordenadores, según el tipo de cable y tipo de conexión.

Conexión a Internet

Para tener acceso a Internet necesitaremos dispositivos hardware (un módem analógico, un módem digital RDSI, un módem ADSL o un cable módem), software (configuración de los protocolos necesarios (TCP/IP) y los programas) y un proveedor de servicios Internet (ISP).

Desde el panel de control seleccionamos Conexiones de red (Tareas de red) y pulsamos en Crear conexión nueva. Seguimos los pasos.

Configuración del cliente de correo electrónico

Configuración desde el programa de Correo que se use

Configuración de una red local

En pequeñas empresas o con fines domésticos lo habitual es crear **redes punto a punto,** también llamadas **grupos de trabajo**. En este modelo, los ordenadores se comunican directamente entre sí y no requieren un servidor. En general, esta red es apropiada para menos de diez equipos conectados con una LAN (Red de Área Local). También podremos modificar la configuración de la red creada posteriormente

Una vez que tenemos instalada y configurada nuestra red podremos compartir carpetas, impresoras y la conexión a Internet. Para las dos primeras deberemos tener el Servicio de red Compartir impresoras y archivos para redes Microsoft instalado. Para la tercera Windows XP proporciona la Conexión compartida a Internet (ICS) que permite conectar un equipo a Internet y después compartir el servicio de Internet con varios equipos conectados a una red.

Además Windows XP ofrece un Servidor de seguridad de conexión a Internet (ICF) para realizar este proceso de protección. En cualquier caso, lo utilizaremos sólo si estamos en una red pequeña y no hemos instalado otros sistemas de seguridad, ni disponemos de un servidor proxy.

Ampliando las posibilidades de la red

Usar archivos de la red sin conexión

A veces puede ser útil tener acceso a archivos de la red sin estar conectados a la misma. Los archivos seleccionados se descargan automáticamente desde carpetas compartidas en la red y se almacenan en nuestro equipo. Cuando estamos desconectados, podemos aún utilizar estos archivos. Cuando volvemos a conectarnos a la red, los cambios se agregan a los archivos de la red en un proceso denominado **sincronización**. Si alguien conectado a la red realiza cambios en el mismo archivo, puede guardar su propia versión, conservar la otra versión o guardar ambas.

Abrimos Mi PC. En el menú Herramientas, seleccionamos Opciones de carpeta. En la ficha Archivos sin conexión, activamos la casilla de verificación Habilitar archivos sin conexión. Seleccionamos Sincronizar todos los archivos sin conexión antes de cerrar la sesión. Después seleccionando el archivo, en el menú Archivo, elegimos Disponible sin conexión

Red Privada Virtual

Sirve para proteger los archivos que se envían. Podemos ampliar nuestra red privada con una conexión de red privada virtual (VPN). En ese caso la conexión a través de Internet está cifrada y es segura. Para ello al crear la red tenemos que seleccionar **Conexión de red privada virtual.**

Conexión a un Escritorio remoto

Esta conexión podrá ser a través de una red local (LAN), una red privada virtual (VPN), o a través de Internet. Es necesario configurar el ordenador al que accederemos (ordenador remoto) y el ordenador desde el que realizaremos el acceso (ordenador cliente). El ordenador remoto deberá ejecutar Windows XP profesional y tener una IP pública conocida por el cliente.

Proceso a realizar en el ordenador remoto. Desde el Panel de control abrimos Sistema y entramos en la ficha Acceso Remoto. En el área Escritorio remoto, pulsamos en Seleccionar usuarios remotos.... Aquí seleccionamos el usuario y la IP Pública para el ordenador cliente.

En el cliente ejecutamos **Conexión a Escritorio remoto** y colocamos el nombre o IP Pública.

Algunos comandos de consola para manejo de redes

- **ping 127.0.0.1:** hace una llamada al ordenador con la IP indicada y espera respuesta.
- **tracert www.microsoft.com:** Realiza una traza desde nuestro ordenador hasta el host indicado (Microsoft) mostrando todos los equipos por los que pasa y el tiempo de respuesta. Es útil para saber en qué equipo se produce un retardo excesivo.
- **ipconfig /all**: Muestra toda la información de nuestro equipo referente a la IP, la máscara, el gateway, dirección física de la tarjeta, etc
- **net view \\servidor:** Muestra la lista de dominios y ordenadores de una red.
- **netstat:** Muestra datos estadísticos de la red, las conexiones activas y los protocolos utilizados.

Seguridad

Uso básico de Perfiles de usuario

Un ordenador puede ser utilizado por varias personas. Windows XP incluye una herramienta de personalización, con la cual, es posible crear cuentas de usuario. Una ventaja es la posibilidad de cambiar de usuario sin reiniciar el ordenador. En Windows XP Profesional podemos utilizar dos menús para gestionar los usuarios,

- uno es más sencillo y limitado (sólo permite crear usuarios locales de mi máquina) y
- el otro permite gestionar grupos de usuarios y definir usuarios pertenecientes a un dominio de una máquina servidora con Windows 2003 por ejemplo.

En una cuenta de usuario local sólo se indican los permisos que el usuario tiene para utilizar los recursos de la máquina específica en que se encuentra, también denominada máquina "local".

Los componentes del perfil de cada usuario quedan almacenados en la carpeta del disco marcado con la letra C denominada Documents and settings. Windows XP Professional ofrece además del Administrador y el Invitado, otros Grupos de Usuarios que permiten definir perfiles más específicos. Todas las cuentas de un mismo grupo compartirán los mismos permisos de seguridad.

- Administradores: No tiene ningún tipo de restricción
- Operadores de copia: Sólo pueden ejecutar servicios con el propósito de realizar copias o restauraciones del sistema.
- Invitados: Está muy restringida en sus permisos
- Operadores de configuración de red: Sólo pueden ejecutar servicios con el propósito de configurar la red.

- Usuarios avanzados: Poseen más derechos administrativos.
- Duplicadores: Permite duplicación de ficheros sin dominio
- Usuarios de escritorio remoto: Tendrán los derechos limitados por la máquina remota a la que se conecten
- Help services group: Es el grupo de la ayuda y servicios de soporte.

Crear discos de contraseñas para usuarios

Si estás ejecutando Windows XP Profesional como usuario local en un entorno de grupo de trabajo, puedes crear un disco de restablecimiento de contraseñas para iniciar la sesión en el ordenador cuando olvides la **contraseña**. También se puede utilizar para no divulgar la contraseña y usar el disco como si fuese una llave de acceso.

Cifrado de datos

En un ordenador suele haber información sensible que debe protegerse para que no sea accesible por cualquier persona, pensemos por ejemplo en contraseñas de acceso, números de cuentas bancarias, informes reservados, etc. Para realizar esta protección el sistema de archivos NTFS incluido en Windows XP ofrece la característica de **seguridad EFS** (Sistema de encriptación de archivos).

Este sistema EFS ofrece la posibilidad de encriptar o cifrar archivos y carpetas. EFS incorpora varios niveles de cifrado para incrementar la seguridad.

- Cada archivo cuenta con una clave de cifrado de archivo única imprescindible para poder descifrar los datos del archivo.
- Esta clave, que también está cifrada, sólo la tienen los usuarios con autorización para ver los datos. Este sistema EFS está integrado con el sistema de archivos NTFS, lo cual dificulta aún más cualquier acceso no autorizado y, al mismo tiempo, facilita la administración a los usuarios.
- Cuando un usuario no autorizado intenta abrir un archivo cifrado sin tener el permiso necesario Windows impedirá su apertura.

Cuando se encripta un solo archivo, será necesario decidir si también se quiere cifrar la carpeta que lo contiene. Si se encripta una carpeta, podremos decidir si todos los archivos y subcarpetas que estén en su interior también se cifrarán. Hay que tener en cuenta que el sistema no permite cifrar algunos tipos de archivos como los comprimidos, los del sistema o los que están en la raíz del sistema de archivos.

Se hace en Propiedades, en la ficha General, en Opciones avanzadas. Activamos la casilla Cifrar contenido para proteger datos. Para descrifrar basta con desactivar la casilla Cifrar contenido para proteger datos

Protección mediante un "cortafuegos" o "firewall"

Para protegernos frente a estos ataques podemos utilizar un **cortafuegos** o **firewall**. Un **servidor de seguridad firewall** es un software o un hardware que crea una barrera protectora entre el equipo y el contenido de Internet potencialmente nocivo. Microsoft Windows XP proporciona un servidor de seguridad conocido como **Servidor de seguridad de conexión a Internet (ICF, Internet Connection Firewall).**

Vamos a “Mis Conexiones de Red” en Propiedades, la pestaña Avanzadas y activamos la casilla Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet.

Herramientas para prevención y solución de problemas

Cuando trabajamos con equipos informáticos debemos tener una política de seguridad, prevención y fiabilidad. El administrador del sistema debe tener un modelo de trabajo que impida perder información valiosa ni puede permitir que la actividad se detenga o ralentice porque se ha producido un fallo.

Copias de seguridad

Deberemos asegurarnos de que tenemos toda la información importante esté guardada en un lugar seguro, para ello, hay que tener un plan completo de copias de seguridad del sistema. Debemos recordar que las copias de seguridad normalmente ocupan bastante espacio por lo que normalmente será necesario utilizar un dispositivo de almacenamiento masivo como una unidad de cinta o un DVD.

Desde el Menú Inicio seleccionamos Programas / Accesorios / Herramientas del sistema / Copia de seguridad, podemos entrar. Podemos escoger entre 5 opciones:

- **Normal o completa:** realiza una copia completa, desactiva el atributo de archivo para todos los copiados. Este tipo de copia ocupa bastante espacio y debe hacerse semanal o mensualmente.
- **Incremental:** copia los archivos creados o modificados desde la última copia de seguridad realizada. Se realiza en combinación con la copia normal y desactiva el atributo de archivo de los copiados. Ocupa menos espacio pero en caso de restauración debo usar la copia normal y todas las incrementales posteriores. Normalmente se hace diariamente.
- **Diferencial:** copia todos los archivos creados o modificados desde la última copia de seguridad completa. También se realiza en combinación con la normal. Para restaurar se usa la copia normal y la diferencial (sólo hay una). No modifica el atributo de archivo. Se suele hacer diariamente.
- **Copia:** copia los archivos seleccionados por el usuario, no modifica el atributo de archivo. El usuario debe controlar cuales son los archivos modificados o nuevos de su ordenador.
- **Diaria:** copia los archivos modificados ese día. No modifica el atributo de archivo.

Herramientas de mantenimiento de las unidades de disco

Windows XP ofrece algunas herramientas de mantenimiento y prevención de fallos

- **Comprobación de errores:** Windows incluye la herramienta **Scandisk** cuyo funcionamiento depende del sistema de archivos que utilicemos FAT, NTFS, etc. Scandisk verifica la integridad de archivos y carpetas y comprueba si hay errores físicos en el disco buscando clusters defectuosos. En Propiedades de la unidad, en la pestaña Herramientas, seleccionamos Comprobar ahora
- **Desfragmentador de discos:** Al almacenar un archivo en el disco duro, éste se guarda en cualquier parte donde haya sitio. Si no se puede encontrar un espacio lo suficientemente grande para almacenar todo el fichero de una sola vez, éste se guarda por fragmentos en diferentes áreas del disco. Se dice entonces que el archivo está **fragmentado**. Cuando hay muchos archivos fragmentados provoca que los programas se ejecuten más despacio y se produzca un mayor desgaste de la unidad del disco duro. El desfragmentador de disco de Windows XP se encarga de comprobar el estado de fragmentación de los archivos del disco duro y posteriormente reordena todos los fragmentos en áreas consecutivas. En Propiedades de la unidad, en la pestaña Herramientas, seleccionamos Desfragmentar ahora

Utilidades de acceso a los archivos de configuración del sistema operativo

La configuración del sistema operativo se almacena en una serie de archivos. Estos archivos pueden ser modificados: por el propio sistema, por distintas aplicaciones y por el administrador del sistema si utiliza la herramienta adecuada. Para ello usamos la aplicación **Msconfig**. Tiene varias partes:

- **Pestaña General:** Inicio normal, inicio con diagnóstico e inicio selectivo
- Pestañas **System.ini, Win.ini y Boot.ini:** permite configurar los parámetros de los archivos de arranque. Algunas funciones de System.ini y Win.ini se realizan ahora desde el Registro de Windows, sin embargo se han mantenido para conservar la compatibilidad
- **Pestaña Servicios** en la que se pueden activar y desactivar los servicios
- **Pestaña Inicio** donde podemos habilitar o deshabilitar los elementos que se van a cargar o no al iniciar Windows.

Además en Menú Inicio / Programas / Accesorios / Herramientas de sistema / Información del sistema, a la izquierda aparece una lista con una completa información tanto hardware como software sobre nuestro equipo.

Restauración del sistema a configuraciones anteriores

Cuando se producen cambios es posible que cometamos errores o que se produzcan incompatibilidades entre los distintos elementos instalados. Como solución a esta situación, Windows ofrece una herramienta que permite restaurar el Sistema Operativo.

Esta herramienta de Restaurar sistema toma una instantánea de los archivos críticos del sistema y de algunos archivos de programa, almacenando esta información como puntos de restauración.

Windows XP crea puntos de restauración automáticamente cuando se producen actualizaciones del sistema o se modifica su restauración, y normalmente cada 24 horas si no se indica lo contrario en las Tareas programadas. Además, en cualquier momento podemos nosotros crear nuevos puntos de restauración

Desde Menú Inicio, seleccionamos Programas / Accesorios / Herramientas de sistema / Restaurar sistema podemos crear una restauración. Si el sistema falla, pulsamos F8 en el menú de arranque y después hacemos clic en Ultima configuración buena conocida. También desde ahí podemos restaurar el sistema.

Complementos de uso avanzado de windows

Algunos atajos de teclado:

- Windows: Despliega en menú Inicio.
- Windows + D: Minimiza o restaura todas las ventanas.
- Windows + E: Muestra el Explorador de Windows.
- Windows + F: Muestra el Buscador de archivos.
- Windows + Ctrl + F: Muestra el Buscador de equipos.
- Windows + F1: Muestra la Ayuda y el Centro de soporte.
- Windows + R: Muestra el cuadro de diálogo Ejecutar.
- Windows + Pausa: Muestra el cuadro de diálogo Propiedades del sistema.
- Windows + Shift + M: Maximiza todas las ventanas.
- Windows + L: Bloquea el equipo.
- Windows + U: Abre el Manager de utilidades.

Algunos comandos sólo pueden ser ejecutados desde una consola o terminal. Para obtener ayuda adicional sobre estos comandos, las opciones que incluye y algunos ejemplos de uso, tan sólo tendremos que añadirle a cada comando la opción /h ó /

Archivos y sistemas de ficheros:

- **cacls:** Permite modificar los permisos en ficheros y carpetas, permitiendo o prohibiendo a cada usuario leer, escribir o modificar el contenido de dichos archivos o carpetas.
- **chkdsk:** Comprueba el estado de una partición y repara los daños en caso de que encuentre alguno. Sin parámetros para chequear la partición, con la opción /F para corrija los errores
- **cipher:** Permite cifrar archivos, directorios o particiones siempre que se encuentren en el sistema de archivos NTFS.
- **comp>:** Compara archivos o carpetas y muestra las diferencias existentes entre ellos.
- **defrag:** Desfragmenta los archivos de una unidad, similar a la utilidad Defragmentador de discos de Windows pero en modo consola.
- **diskpart:** Permite crear, eliminar y administrar particiones. Debemos usarlo con cuidado ya que es fácil que eliminemos una partición sin darnos cuenta
- **find y findstr:** Estos comandos buscan cadenas de textos en el interior de uno o varios archivos. El comando findstr ofrece más opciones de búsqueda
- **iexpress:** Este comando lanzará un asistente para crear archivos comprimidos .CAB autodescomprimibles.

Configuración del sistema:

- **bootcfg:** permite ver y modificar las entradas del archivo boot.ini.
- **control userpasswords2:** permite modificar las claves y los permisos de los diferentes usuarios, así como requerir la pulsación de control+alt+suprimir para poder iniciar sesión, haciendo el inicio de sesión más seguro.
- **msconfig:** Podemos seleccionar los programas y servicios que se cargan durante el inicio de Windows así como los sistemas operativos que el usuario puede seleccionar para iniciar el ordenador.
- **regedit:** Editor del registro en modo gráfico.
- **sfc:** Permite buscar archivos del sistema dañados y recuperarlos en caso de que estén defectuosos (es necesario el CD de instalación del sistema operativo para utilizarlo). Para realizar una comprobación inmediata, deberemos ejecutar la orden sfc /scannow.
- **systeminfo:** Muestra información sobre nuestro equipo y nuestro sistema operativo: número de procesadores, tipo de sistema, actualizaciones instaladas, etc.
- **taskkill:** Permite eliminar un proceso conociendo su nombre o el número del proceso (PID).
- **tasklist:** Realiza un listado de todos los procesos que hay. Útil si deseamos eliminar un proceso y no conocemos exactamente su nombre o su PID.

Redes:

- **arp:** Muestra y permite modificar las tablas del protocolo ARP, encargado de convertir las direcciones IP de cada ordenador en direcciones MAC
- **ftp:** Permite conectarse a otra máquina a través del protocolo FTP para transferir archivos.
- **getmac:** Muestra las direcciones MAC de los adaptadores de red que tengamos instalados en el sistema.
- **ipconfig:** Muestra y permite renovar la configuración de todos los interfaces de red.
- **nbtstat:** Muestra las estadísticas y las conexiones actuales del protocolo NetBIOS sobre TCP/IP, los recursos compartidos y los recursos que son accesibles.
- **net:** Permite administrar usuarios, carpetas compartidas, servicios, etc. Para un listado

completo de todas las opciones, escribir net sin ningún argumento. Para obtener ayuda sobre alguna opción en concreto, escribir net help opción.
- **netsh:** permite ver, modificar y diagnosticar la configuración de la red
- **netstat:** obtendremos un listado de todas las conexiones de red que nuestra máquina ha realizado.
- **nslookup:** Esta aplicación se conecta a nuestros servidores DNS para resolver la IP de cualquier nombre de host.
- **pathping:** Muestra la ruta que sigue cada paquete para llegar a una IP determinada, el tiempo de respuesta de cada uno de los nodos por los que pasa y las estadísticas de cada uno de ellos.
- **ping:** Poniendo el nombre o la dirección IP de la máquina enviaremos un paquete a la dirección que pongamos para comprobar que está encendida y en red.
- **rasdial:** Permite establecer o finalizar una conexión telefónica.
- **route:** Permite ver o modificar las tablas de enrutamiento de red.
- **tracert:** muestra el camino seguido para llegar a una IP y el tiempo de respuesta de cada nodo.

Otras:

- **logoff:** cierra una sesión iniciada en nuestro ordenador o en otro ordenador remoto.
- **msg:** Envía un mensaje a unos o varios usuarios determinados mediante su nombre de inicio de sesión o el identificador de su sesión
- **runas:** ejecuta un programa con privilegios de otra cuenta. Útil por ejemplo si estamos como usuario limitado y queremos hacer algo que necesite privilegios de administrador.
- **shutdown:** Permite apagar, reiniciar un ordenador o cancelar un apagado. Es especialmente útil si hemos sido infectados con el virus Blaster o una de sus variantes para cancelar la cuenta atrás. Para ello, tan sólo tendremos que utilizar la sintaxis shutdown -a.

Microsoft Management Console (MMC)

Estos comandos nos darán acceso a la aplicación Microsoft Management Console, que proporciona un conjunto de pequeñas utilidades que nos permitirán controlar parte de la configuración de nuestro sistema operativo.

- **compmgmt.msc:** Da acceso a la Administración de equipos, desde donde podemos configurar nuestro ordenador y acceder a otras partes de la MMC.
- **devmgmt.msc:** Accede al Administrador de dispositivos.
- **dfrg.msc:** Desfragmentador del disco duro.
- **diskmgmt.msc:** Administrador de discos duros.
- **fsmgmt.msc:** Permite administrar y monitorizar los recursos compartidos.
- **gpedit.msc:** Permite modificar las políticas de grupo.
- **lusrmgr.msc:** Permite ver y modificar los usuarios y grupos locales.
- **ntmsmgr.msc:** Administra y monitoriza los dispositivos de almacenamientos extraíbles.
- **perfmon.msc:** Monitor de rendimiento del sistema.
- **services.msc:** Administrador de servicios locales.

Servicios

Los servicios son programas o aplicaciones cargadas por el propio sistema operativo y que se ejecutan en segundo plano (Background). Para visualizar los servicios y modificar su configuración debemos abrir una aplicación de gestión denominada consola de servicios. Una vez en la consola, hacemos clic con el botón derecho sobre el servicio que queremos iniciar o detener y modificamos su estado con Detener o Iniciar.

Los servicios pueden encontrarse en dos estados posibles:

- iniciados, es decir, se encuentra ejecutándose, o
- pueden estar detenidos.

Además tenemos tres opciones posibles de inicio:

- Automático: Se inician junto con el sistema operativo.
- Manual: Podemos iniciarlo y detenerlo manualmente cuando queramos, además, otro servicio puede hacerlo automáticamente. En un principio estaría detenido.
- Deshabilitado: No se puede iniciar manualmente ni otro servicio puede hacerlo.

Algunos servicios del sistema interesantes:

- **Actualizaciones automáticas.** Se utiliza para chequear automáticamente si salió algún nuevo parche o actualización del sistema operativo Windows de Microsoft.
    - Nombre en Inglés: Automatic Updates (wuauserv)
    - Ejecutable o DLL: svchost.exe
- **Portafolios:** Por defecto, la información que copiamos o cortamos es trasladada al portapapeles (Clipboard) y permanece ahí, hasta que copiemos o cortemos nuevamente. Si habilitamos este servicio, podremos compartir esta información con otras personas que tengan el Visor de Portafolios (ClipBook Viewer) instalado en su ordenador y viceversa. Se recomienda Deshabilitarlo
    - Nombre en Inglés: ClipBook (ClipSrv)
    - Ejecutable o DLL: clipsrv.exe
- **Cliente DHCP:** permite la asignación dinámica y automática de direcciones IP. Se recomienda Manual si nuestra máquina no forma parte de ninguna red o tenemos un IP estático o fijo. De lo contrario, o si nos conectamos a Internet a través de un módem necesitamos que este servicio esté en Automático.
    - Nombre en Inglés: DHCP Client (DHCP)
    - Ejecutable o DLL: svchost.exe
- **Cliente DNS:** Resuelve y almacena los nombres DNS (Domain Name System) para este equipo. Si la máquina está en red, Automático. De lo contrario Manual. Requerido si usas IPSEC.
    - Nombre en Inglés: DNS Client (Dnscache)
    - Ejecutable o DLL: svchost.exe
- **Servicio de informe de errores:** Se utiliza para informar a Microsoft cuando ocurre algún error en una aplicación o servicio que se ejecuta en un modo no estándar. Es conveniente Deshabilitarlo
    - Nombre en Inglés: Error Reporting Service (ERSvc)
    - Ejecutable o DLL: svchost.exe
- **Ayuda y soporte técnico:** Habilita el centro de Ayuda y Soporte técnico (Help and Support Center) en este equipo. Se recomienda poner de manera Manual. Y habilitar sóo cuando se necesite.
    - Nombre en Inglés: Help and Support (helpsvc)
    - Ejecutable o DLL: svchost.exe
- **Conexión de seguridad a Internet (ICF) / Conexión compartida a Internet (ICS):** se utiliza para compartir la conexión a Internet. Debe estar Automático si compartimos la conexión o requerimos del Firewall de Windows XP. De lo contrario Deshabilitado.
    - Nombre en Inglés: Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS) (SharedAccess)
    - Ejecutable o DLL: svchost.exe
- **Cola de impresión.** Se encarga de poner los archivos a imprimir en la cola de espera. Este servicio es requerido si utilizamos impresoras, incluso las que están en red. Se recomienda tener en modo Automático, salvo que no necesitemos imprimir.
    - Nombre en Inglés: Print Spooler (Spooler)
    - Ejecutable o DLL: spoolsv.exe

- **Servicio de restauración de sistema:** se encarga de monitorear cambios en archivos de sistema y algunas aplicaciones para así registrar o guardar versiones anteriores y crear un punto de restauración.
    - Nombre en Inglés: System Restore Service (srservice)
    - Ejecutable o DLL: svchost.exe
- **Horario de Windows.** Automáticamente ajusta el reloj de nuestra máquina conectándose a servidores de Internet.
    - Nombre en Inglés: Windows Time (W32Time)
    - Ejecutable o DLL: svchost.exe

13. Administración y configuración de Windows 2000/2003 server

Windows como sistema operativo servidor

Microsoft abrió una línea de productos diseñada para actuar como verdaderos sistemas operativos de red, esto es servidores de red. En los cuales se incorporaran cualidades tales como:

- Gestión centralizada de usuarios y grupos.
- Capacidad de proveer servicios de red como DHCP, Web, correo electrónico, DNS, etc.
- Implementación de sistemas de seguridad, robustez, fiabilidad y recuperación de fallos.
- Posibilidad de ofrecer servicios de red privada virtual (VPN).
- Acceso remoto.
- Posibilidad de actuar como servidor de archivos e impresión.

El **primer producto** de esta clase fue **Windows NT Server**, que supuso una revolución y que fue rápidamente adoptado como un buen sistema operativo servidor. Más tarde Windows NT Server fue **sustituido por Windows 2000 Server** y hoy día se encuentra disponible la última versión, **Windows 2003 Server.** Este tiene varias ediciones:

- **Microsoft Windows Server 2003 standard edition**: Ésta es la edición más habitual para empresas pequeñas y medianas. Puede soportar hasta 4 procesadores y es capaz de manejar hasta 4Gb de memoria RAM.
- **Microsoft Windows Server 2003 enterprise edition**: Diseñada para satisfacer las necesidades de grandes empresas. Hasta 8 procesadores y hasta 64 Gb de RAM. Soporta **clustering** (Técnica que consiste en agrupar varios ordenadores que aparentan ser uno sólo que tiene la potencia de todos juntos). Está disponible en versiones de 32 y 64 bits para aprovechar la potencia de los procesadores.
- **Microsoft Windows Server 2003 datacenter edition**: Hasta 64 procesadores en paralelo y versiones de 32 y 64 bits. El Windows 2003 Server más avanzado en cuanto a escalabilidad, fiabilidad y rendimiento.
- **Microsoft Windows Server 2003 Web edition**: Especialmente diseñado para funcionar como servidor de aplicaciones Web.

Las redes en Windows 2000/2003 Server

Microsoft plantea dos modelos o esquemas de funcionamiento en red.

- **Modelo de trabajo en grupo:** Un grupo de trabajo es un conjunto de equipos en red que comparte recursos, como ficheros o impresoras. También se llama una **red de igual a igual** (peer to peer), porque todos comparten recursos por igual sin un servidor dedicado. Cada equipo en el grupo de trabajo tiene una base de datos local de seguridad con, una lista de cuentas de usuario para el equipo en la que reside. La administración de cuentas de usuario y recursos de seguridad está **descentralizada**. Esto reduce las labores de planificación y administración de la red. En redes pequeñas (hasta 10 ordenadores) y con bajos requerimientos de rendimiento o seguridad, este modelo puede ser suficiente. Las desventajas son:
    - Un usuario debe tener una cuenta en cada equipo al que quiera tener acceso.
    - Cualquier cambio en las cuentas de usuario se debe realizar en cada equipo del grupo de trabajo.

    - La administración de los recursos compartidos (archivos e impresoras) se hace individualmente en cada equipo y por los usuarios individuales que tienen cuentas en esos equipos. Lo que no favorece la seguridad y hace muy laboriosa la administración.

- **Modelo de dominios:** Un dominio es una agrupación de redes de ordenadores que comparten una base de datos de un directorio central. En Windows 2000 y 2003 Server, la base de datos que tiene toda la información del dominio, sus servicios, y recursos se llama **Active Directory** (diferencia principal con NT). El directorio está situado en el equipo que está configurado como controlador de dominio. Un **controlador de dominio** es un ordenador servidor con sistema operativo Windows 2000/2003 Server que gestiona todos los aspectos relativos a la seguridad en las interacciones de los usuarios del dominio. La seguridad y la administración están **centralizadas**. El controlador siempre será Windows 2000/2003 Server aunque otros sistema pueden ser miembros del dominio. Las ventajas son:
    - Un dominio permite una administración centralizada, porque toda la información de usuarios se almacena centralmente.
    - Un dominio proporciona un proceso único de entrada al sistema, para que los usuarios puedan acceder a los recursos de red, como archivos, impresoras y recursos de aplicaciones para los que tengan permiso.
    - Un dominio proporciona escalabilidad, de manera que el administrador puede crear redes que van aumentando de tamaño y prestaciones con el paso del tiempo y a medida que surgen necesidades.

  En un dominio se pueden encontrar las siguientes clases de ordenadores:
    - Controladores de dominio con Windows 2000/2003 Server. Cada controlador de dominio almacena y mantiene una copia del directorio. Cuando hay varios controladores de dominio, replican periódicamente su información de directorio sincronizándola.
    - Servidores miembro con Windows 2000/2003 Server. Son equipos que sirven algún recurso a los demás pero no tienen copia del directorio. Por ejemplo proporcionan recursos compartidos como carpetas o impresoras.
    - Equipos cliente. Los equipos cliente tienen un entorno de escritorio para el usuario que les permite acceder a los recursos del dominio. Se puede instalar cualquiera de las versiones de sistemas operativos Windows

Servicios de directorio en Windows 2000/2003 Server. Active Directory

La base de esa centralización la constituye el directorio, lo que Microsoft denomina Directorio Activo (Active Directory). Este elemento se introdujo a partir de Windows 2000 Server y supuso un gran cambio con respecto a versiones anteriores (Windows NT).

- Active Directory proporciona un método para el diseño de la estructura de directorio que responde a las necesidades de cualquier organización. Posee numerosas ventajas, como por ejemplo la **escalabilidad del sistema y la facilidad para localizar recursos** a lo largo de una gran red.
- Active Directory permite **un punto único de administración** para todos los recursos públicos, entre los que se pueden incluir archivos, dispositivos periféricos, conexiones a bases de datos, accesos Web, usuarios, servicios, etc. Utiliza el DNS de Internet como servicio de localización.

- Active Directory utiliza componentes para construir una estructura de directorio acorde con las necesidades de una organización. La estructura lógica de la organización se representa por medio de dominios, unidades organizativas, árboles y bosques. La estructura física está representada por sitios (subredes físicas) y controladores de dominio. Active Directory **separa completamente la estructura lógica de la física**.

Dividimos dos tipos de estructuras:

- **Estructuras lógicas:** los recursos presentan una estructuración que refleja la estructura lógica de la organización donde está instalado. Agrupar recursos lógicamente permite encontrar un recurso por su nombre en vez de por su localización física. Las estructuras lógicas son:
    - **Dominio**: La unidad central de la estructura lógica de Active Directory es el dominio, que puede almacenar millones de objetos. Los objetos que se almacenan en un dominio son por ejemplo: impresoras, documentos, direcciones de correo electrónico, bases de datos, usuarios, etc. Todos los objetos de la red existen en un dominio, y cada dominio almacena información exclusivamente sobre los objetos que contiene. Active Directory está compuesto por uno o más dominios. Un dominio contiene listas de control de acceso (ACL-Access Control List), éstas controlan el acceso a los objetos del dominio. Las ACL contienen los permisos asociados con los objetos que controlan los usuarios que pueden acceder a un objeto.
    - **Unidad organizativa:** Una unidad organizativa (OU-Organizational Unit) es un contenedor que se utiliza para organizar objetos dentro de un domino en grupos que reflejan la estructura funcional de una organización. Por ejemplo, un dominio miempresa.com puede contener tres OU: ventas, pedidos y contabilidad.
    - **Árbol:** Es una agrupación o una ordenación jerárquica de uno o más dominios de Windows 2000/2003 que se pueden crear añadiendo uno o más dominios secundarios a un dominio principal existente.
    - **Bosque**: Un bosque es una agrupación o configuración jerárquica de uno o más árboles de dominio distintos y completamente independientes entre sí.

- **Estructuras físicas:** Los componentes físicos de Active Directory son:
    - **Sitio:** es una combinación de una o más subredes que utilizan IP (Internet Protocol) conectadas por un enlace rápido y de alta fiabilidad que permite agrupar la mayor cantidad de tráfico posible. Normalmente un sitio será una red de área local (LAN).
    - **Controlador de dominio:** es un equipo con Windows 2000/2003 Server que almacena una copia del directorio de dominio (base de datos local del dominio). Dado que un dominio puede contener uno o más controladores de dominio, todos los controladores de dominio en un dominio tienen una copia completa del directorio. Cada controlador de dominio almacena una copia completa de toda la información de Active Directory para ese dominio, administra los cambios y replica (extiende) esos cambios a otros controladores de dominio del mismo dominio. El hecho de tener más de un controlador de dominio en un dominio es importante porque provee tolerancia a fallos. Si un controlador de dominio está desconectado, otro controlador de dominio puede proporcionar todas las funciones necesarias.

Instalación de Windows 2000/2003 Server

La instalación de un sistema Windows 2000/2003 Server debería comenzar con una planificación cuidadosa de nuestra red y nuestra organización.

- **Requisitos del sistema:** Lo primero que deberíamos hacer es comprobar si el hardware que vamos a utilizar es compatible con Windows 2000/2003 Server. Microsoft proporciona en la carpeta Support del CD de instalación una lista de hardware compatible (HCL, Hardware Compatibility List).

- **Planificación de las particiones:** dividir en particiones y configurar las unidades de almacenamiento. Microsoft recomienda utilizar el sistema de archivos NTFS ya que posee muchas ventajas, como eficiencia, fiabilidad, seguridad y compresión, además para utilizar el servidor como controlador de dominio o servidor de Active Directory debe estar en una partición NTFS. Por regla general, se utilizarán una o más unidades de disco para datos, preferiblemente configuradas con algún sistema de tolerancia a fallos como RAID.
- **Recogida de información de la red:** hay que decidir los siguientes parámetros:
    - **Nombre en el Sistema de nombres de dominio del equipo:** Este nombre puede contener letras mayúsculas o minúsculas, números y el carácter guión. El nombre DNS del servidor no debe sobrepasar los 15 caracteres si se pretende que el nombre NetBIOS sea el mismo que el DNS y mantener así la compatibilidad con clientes que no sean Windows 2000/2003.
    - **Nombre del dominio o grupo de trabajo al que debe unirse (si se encuentra en una red):** Si se está creando un nuevo dominio Windows 2000/2003, este nombre debería ser compatible con el DNS: por ejemplo: midepartamento.miempresa.com.
    - **Dirección IP del equipo:** necesario salvo que la red disponga de un servidor de Protocolo de Configuración Dinámica de Host (DHCP, Dynamic Host Configuration Protocol).
    - **Modo de licencia de clientes y el número de clientes simultáneosTeclados, monitores y ratones (si el modo de licencia es Por servidor)** Windows 2000/2003 Server soporta licencias "Por servidor" y "Por puesto". Si no se está seguro de qué modo de licencia utilizar, es mejor elegir "Por servidor". Se puede cambiar de modo "Por servidor" a "Por puesto" una vez (sin coste adicional) pero no de modo "Por puesto" a modo "Por servidor".
- **Instalación de Windows 2000 Server. Primera parte (modo texto):** Cuando se inicia desde el CD-ROM se entra en la fase de instalación basada en texto en la cual el programa de instalación copia los archivos necesarios para reiniciar en Windows 2000 para la parte de instalación basada en interface gráfico.
- **Instalación de Windows 2000 Server. Segunda parte (modo gráfico):** Cuando la fase basada en texto de la instalación concluya, el equipo se reiniciará y Windows 2000 se iniciará por primera vez, cargando el Asistente para la instalación de Windows 2000.

Directorio Activo (Active Directory).

Una vez que haya concluido una instalación de Windows 2000 Server es el momento de instalar, configurar y administrar el servicio de directorio activo (Active Directory). Cuando se tiene un sistema Windows 2000 recién instalado el directorio activo no se encuentra en uso.

Para **instalar el Primer controlador de dominio** deberemos seguir los siguientes pasos:

- **Iniciar** la Herramienta Configuración del Servidor desde el menú de Herramientas Administrativas.
- **Tipo de Controlador de Dominios:** Si el servidor ya es un controlador de dominio, el asistente solo proporciona la opción de degradar el sistema de nuevo a servidor independiente o miembro. En un equipo que no es un controlador de dominio, el asistente muestra la pantalla Tipo de controlador de dominios, pidiendo que se seleccione:
    - Controlador de dominio para un nuevo dominio: Instala Active Directory en el servidor y lo designa como el primer controlador de dominio de un nuevo dominio.
    - Controlador de dominio adicional para un dominio existente: Instala Active Directory en el servidor y replica la información del directorio desde un dominio existente.
- **Crear árbol o dominio secundario.** Deberemos elegir el tipo de dominio que queremos configurar de las dos opciones que se presentan en el siguiente cuadro.
    - Crear un nuevo árbol de dominios: Configura el nuevo controlador de dominio para

que aloje el primer dominio de un nuevo árbol.
    - Crear un nuevo dominio secundario en un árbol de dominios existente: Configura el nuevo controlador de dominio para que aloje un hijo de un dominio de un árbol que ya existe.
- **Crear o unir bosque,** que permite especificar una de las siguientes opciones:
    - Crear un nuevo bosque de árboles de dominios: Configura el controlador de dominio para que sea la raíz de un nuevo bosque de árboles.
    - Situar este nuevo árbol de dominios en un bosque existente: Configura el controlador de dominio para que aloje el primer dominio de un nuevo árbol en un bosque que ya contiene uno o más árboles.
- **Nombre de nuevo Dominio:** Para identificar el controlador de dominio en la red se debe especificar un nombre DNS valido para el dominio que se está creando. Este nombre no tiene por qué ser el mismo que el del dominio de Internet que utiliza la empresa u organización donde se está instalando Windows 2000/2003 Server (aunque puede serlo).
- **Nombre de dominio NetBIOS:** Después de introducir un nombre DNS para el dominio, el sistema solicita un equivalente NetBIOS para el nombre del dominio para que los utilicen los clientes que no soporten Active Directory. Windows NT 4 y los sistemas Microsoft Windows 95/98 utilizan nombres NetBIOS para todos los recursos de la red, incluyendo los dominios. Si se dispone de clientes de nivel inferior en la red (esto es, Windows NT 4, Windows 95/98, Microsoft Windows para Trabajo en grupo o Cliente de red Microsoft para sistemas MS-DOS), estos sólo serán capaces de ver el nuevo dominio por medio del nombre NetBIOS.
- **Ubicación de la base de datos de Active Directory:** La base de datos de Active Directory contendrá los objetos Active Directory y sus propiedades. La ubicación predeterminada tanto para la base de datos como para los registros es la carpeta %SystemRoot%\Ntds del volumen del sistema, pero se pueden modificar
- **Volumen del sistema compartido:** Permite especificar la ubicación de lo que se convertirá en el recurso compartido Sysvol del controlador de dominio. El volumen del sistema es un recurso compartido que contiene información del dominio que se replica al resto de controladores de dominio de la red. De forma predeterminada, el sistema crea este recurso compartido en la carpeta %SystemRoot%\Sysvol en la unidad de disco del sistema.
- **Instalación de DNS:** En este punto, el Asistente para instalación de Active Directory tiene toda la información de configuración necesaria para instalar Active Directory y promover el servidor a controlador de dominio.
- **Finalización de la instalación de Active Directory:** Después de que el asistente contacte con el servidor DNS que proporcionara el servicio localizador para el nuevo dominio, se completa la instalación y configuración de Active Directory sin más introducción de datos por parte del usuario. El asistente registra todas las actividades que se producen durante el proceso de instalación en dos archivos llamados Dcpromo.log y Dcpromoui.log, localizados en la carpeta %SystemRoot%\debug. Finalmente hay que reiniciar el sistema

La herramienta básica para **administración de los dominios** es el complemento Usuarios y equipos de Active Directory. Para usarla es necesario iniciar sesión en el dominio utilizando una cuenta que tenga privilegios administrativos.

El cuadro de diálogo principal de **Usuarios y equipos de Active Directory** contiene muchos de los elementos estándar de las pantallas de la MMC. El árbol de la consola (a la izquierda) muestra un dominio Active Directory y los objetos contenedor dentro de una pantalla expandible. El panel de resultados (a la derecha) muestra los objetos del contenedor resaltado. Los objetos de la pantalla Usuarios y equipos de Active Directory representan tanto entidades físicas (equipos y usuarios), como las entidades lógicas (grupos y unidades organizativas).

- **Dominio:** Objeto raíz de la pantalla Usuarios y equipos de Active Directory; identifica el dominio que está administrando actualmente el administrador.
- **Unidad organizativa:** Objeto contenedor utilizado para crear agrupaciones lógicas de

objetos equipo, usuario y grupo.

- **Usuario:** Representa un usuario de la red y funciona como un almacén de información de identificación y autenticación.
- **Equipo:** Representa un equipo de la red y proporciona la cuenta de máquina necesaria para que el sistema inicie sesión en el dominio.
- **Contacto:** Representa un usuario externo al dominio para propósitos específicos como envío de correo electrónico; no proporciona las credenciales necesarias para iniciar sesión en el dominio.
- **Grupo:** Objeto contenedor que representa una agrupación lógica de usuarios, equipos u otros grupos (o los tres) que es independiente de la estructura del árbol de *Active Directory*. Los grupos pueden contener objetos de diferentes unidades organizativas y dominios.
- **Carpeta compartida:** Proporciona acceso de red, basado en *Active Directory*, a una carpeta compartida en un sistema Windows 2000.
- **Impresora compartida**: Proporciona acceso de red, basado en *Active Directory*, a una impresora compartida en un sistema Windows 2000.

Usuarios

Cada persona que tenga acceso al sistema necesitará una cuenta de usuario. Una cuenta de usuario hace posible:

- Autentificar la identidad de la persona que se conecta a la red.
- Controlar el acceso a los recursos del dominio.
- Auditar las acciones realizadas utilizando la cuenta.

Windows 2000 sólo crea dos cuentas predefinidas:

- la cuenta Administrador, que otorga al usuario todos los derechos y permisos,
- y la cuenta Invitado, que tiene derechos limitados.
- El resto de las cuentas las crea un administrador y son cuentas de dominio (válidas a lo largo de todo el dominio de forma predeterminada) o cuentas locales (utilizables sólo en la máquina donde se crean).

Una cuenta de usuario tiene muchas propiedades entre ellas:

- Pestaña Perfil: Muestra la ruta de acceso al perfil del usuario, la ruta de acceso de cualquier archivo de comandos que se ejecuta en el inicio de sesión, la ruta de acceso al directorio principal y cualquier conexión automática de unidades.
- Pestaña Miembro de: Enumera las pertenencias a grupos del usuario. Aquí se pueden especificar a qué grupos está adscrito el usuario.

En los ordenadores cliente de una red basada en Windows 2000/2003 Server habrá que especificar que el inicio de sesión se haga en un dominio y no en modo local. Esto quiere decir que el usuario y contraseña no se comprobarán en forma local, sino contra la base de datos de Active Directory del controlador de dominio.

Gestión y Directivas de Grupos

Por definición, los grupos en Microsoft Windows 2000/2003 Server son objetos del servicio de directorio Active Directory o del equipo local que pueden contener usuarios, equipos y otros grupos. Sin embargo, en general, un grupo es normalmente una colección de cuentas de usuario. El objetivo de los grupos es simplificar la administración. En Windows 2000 hay tres tipos de grupos:

- **Grupos locales:** Los grupos locales se definen en un equipo local. Se utilizan solamente en el equipo local.
- **Grupos de Seguridad:** Los grupos pueden tener descriptores de seguridad asociados con ellos.
- **Grupos de distribución:** Los grupos se utilizan para las listas de distribución de correo electrónico. No pueden tener descriptores de seguridad asociados.

Cuando se crea un grupo, se le asigna un ámbito de grupo que define cómo se asignaran los permisos. Las tres posibilidades de ámbitos de grupo son:

- **Dominio Local:** Se utilizan para garantizar permisos dentro de un único Dominio. Los miembros de los grupos de dominio local pueden incluir solamente cuentas, tanto de usuarios como de grupos y grupos del dominio en el que se definen.
- **Global:** Se utilizan para otorgar permisos a objetos en cualquier dominio en el árbol de dominio o en el bosque. Los miembros de los grupos globales pueden incluir solamente cuentas y grupos del dominio en el que están definidos.
- **Universal:** Se utilizan para otorgar permisos a gran escala en el árbol de dominio o en el bosque. Los miembros de los grupos universales son las cuentas y grupos de cualquier dominio en el árbol de dominio o en el bosque.

Existen una serie de **grupos locales predefinidos**:

- **Administradores:** Sus miembros pueden realizar todas las tareas administrativas en el equipo. La cuenta predefinida Administrador que se crea cuando se instala el sistema operativo es un miembro del grupo.
- **Invitados:** Sus miembros sólo pueden realizar tareas para las cuales el administrador haya concedido permisos.
- **Operadores de copia:** Sus miembros pueden iniciar sesión en el equipo, hacer copia de seguridad y recuperar la información del equipo y apagar el equipo. No hay miembros predeterminados en el grupo.
- **Usuarios:** Los miembros de este grupo pueden iniciar sesión en el equipo, acceder a la red, almacenar documentos y apagar el equipo. Los miembros no pueden instalar programas o hacer cambios en el sistema. Cuando un servidor miembro o una máquina Windows 2000 Profesional se une a un dominio, el grupo Usuarios del dominio se añade a este grupo.
- **Usuarios avanzados:** Sus miembros pueden crear y modificar cuentas de usuario e instalar programas en el equipo local pero no pueden ver los archivos de otros usuarios.

Los grupos locales de dominio predefinidos de Windows 2000 proporcionan a los usuarios derechos y permisos para realizar tareas en controladores de dominio y en el Active Directory. **Grupos locales de dominio predefinidos** usados más frecuentemente

- **Administradores:** Sus miembros tienen concedido automáticamente cualquier derecho o permiso de todos los controladores de dominio y del propio dominio. La cuenta Administrador, el grupo Administración de empresas y el grupo Admins. del dominio son miembros.
- **Invitados:** Sus miembros sólo pueden realizar tareas para las cuales el administrador haya concedido permisos. Los grupos Usuarios invitados a Invitados de dominio son miembros de forma predeterminada.

- **Operadores de copia:** Sus miembros pueden hacer copia de seguridad y recuperar información en todos los controladores de dominio utilizando Copia de seguridad de Windows 2000.
- **Operadores de cuentas:** Sus miembros pueden crear, eliminar y gestionar cuentas y grupo de usuarios. Los miembros no pueden modificar el grupo Administradores o cualquiera de los grupos Operadores.
- **Operadores de impresión:** Sus miembros pueden gestionar todos los aspectos de la operación y configuración de impresoras en el dominio.
- **Operadores de servidores:** Sus miembros pueden realizar la mayoría de las tareas administrativas en los controladores de dominio, excepto la manipulación de las opciones de seguridad.
- **Usuarios:** Sus miembros pueden iniciar sesión en el equipo, acceder a la red, almacenar documentos y apagar el equipo. Los miembros no pueden instalar programas o hacer cambios en el sistema. El grupo Usuarios del dominio es miembro de este grupo de forma predeterminada.

Los grupos globales predefinidos se crean para englobar tipos de cuentas comunes. De forma predeterminada, estos grupos no tienen derechos heredados. **Grupos globales predefinidos** usados más frecuentemente

- **Administración de empresas:** Este grupo es para usuarios que tengan derechos administrativos en toda la red. Administración de empresas es automáticamente un miembro del grupo local de dominio Administradores en el dominio en el que se creo. Será necesario añadirlo al grupo local de dominio Administradores de otros dominios.
- **Administradores del dominio:** Este grupo es automáticamente un miembro del grupo local de dominio Administradores, por lo que los miembros de Administradores del dominio pueden realizar tareas administrativas en cualquier equipo del dominio. La cuenta Administrador es un miembro de este grupo de forma predeterminada.
- **Controladores del dominio:** Todos los controladores de dominio del dominio son miembros.
- **Equipos del dominio:** Son miembros todos los controladores y estaciones de trabajo del dominio.
- **Invitados del dominio:** La cuenta Invitado es un miembro de forma predeterminada. Este grupo es automáticamente un miembro del grupo local de dominio Invitados.
- **Propietarios del creador de directivas de grupo:** Sus miembros pueden crear y modificar la directiva de grupo del dominio.
- **Usuarios del dominio:** Todos los usuarios del dominio y la cuenta Administrador son miembros. El grupo Usuarios del dominio es automáticamente un miembro del grupo local de dominio usuarios.

Servicios de Terminal Server

En una red grande y que está compuesta por ubicaciones distantes entre sí, es muy necesaria una forma de acceder de forma remota al servidor. También ocurre que a veces los usuarios necesitan ejecutar aplicaciones que están instaladas en el servidor. Para estas situaciones Windows 2000/2003 Server ofrece el servicio de **Terminal Server.** Servicios de Terminal Server de Windows aporta a Windows capacidad multiusuario verdadera. Cada usuario que se conecta a un servidor de Windows 2000/2003 Server mediante Terminal Server de Windows utiliza en realidad los recursos del propio servidor, no los del ordenador concreto en la que está trabajando. Cada usuario obtiene su propia sesión de Servicios de Terminal Server de Windows, y cada sesión está completamente aislada de las demás sesiones del mismo servidor.
Las **ventajas** de utilizar *Terminal Server* son:

- **Acceso remoto:** *Terminal Server* ofrece la solución para que los usuarios puedan ejecutar aplicaciones a través por ejemplo de la línea telefónica a través de un MODEM.

- **Gestión centralizada:** Como todas las aplicaciones de una sesión de Servicios de *Terminal Server* de Windows se ejecutan en el servidor, la gestión de las sesiones y de las aplicaciones se simplifica enormemente.
- **Administración remota:** Al configurarse en el modo de administración remota, Servicios de *Terminal Server* de Windows puede utilizarse también como herramienta de administración.

En todos los equipos cliente será necesario instalar el **cliente para Terminal Server**

Copias de seguridad

Lo primero es decidir en qué medio físico se pretenden almacenar los datos. En Windows 2000/2003 se pueden utilizar cintas magnéticas, pero también se permite copiar los datos en un archivo de copia de seguridad existente en cualquier dispositivo al que se pueda acceder por el sistema, esto incluye discos compactos (como las unidades de Iomega Zip y Jazz), discos duros o incluso grabadoras de CD-ROM.

Una **estrategia** para la copia de seguridad debería tener en cuenta los siguientes aspectos:

- ¿Cuánta información se debe copiar?
- ¿De cuánto tiempo se dispone para realizar la copia de seguridad?
- ¿Cada cuánto tiempo se debe realizar una copia de seguridad de la información?
- ¿Quién se encarga de verificar el acabado de las copias de seguridad?
- ¿Cuántas cintas (u otros medios) se planea utilizar?
- ¿Cada cuánto tiempo se rescribirán las cintas (u otros medios)?

La mayoría de los tipos de copia de seguridad se basan en el **atributo de archivo** para determinar cuándo han cambiado los archivos de un disco concreto y deben ser copiados de nuevo. El atributo de archivo en Windows 2000/2003 es el mismo que el de MS-DOS, independientemente del sistema de archivos que se utilice. El atributo es un único bit que se incluye en la descripción de cada archivo y que el software de copia de seguridad se encarga de marcar o borrar cuando se necesita.

- **Copia de seguridad normal:** una copia de seguridad total de todos los archivos y directorios seleccionados en el software de Copia de seguridad de Windows 2000.
- **Copia de seguridad incremental:** el programa examina el bit de modificado y hace una copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad incremental o normal. Al igual que con la copia de seguridad normal, esta tarea borra el bit de modificado de cada archivo que copia.
- **Copia de seguridad diferencial:** es lo mismo que una copia de seguridad incremental exceptuando que el programa no elimina el bit de modificación de los archivos que copia al medio físico. Esto significa que durante una copia de seguridad diferencial se copian todos los archivos que han cambiado desde la última copia de seguridad normal o incremental. Cuando se realiza una restauración, se necesitan sólo los archivos de copia de seguridad normal y el más reciente de tipo diferencial.

Una estrategia de copia de seguridad de red utilizará normalmente, además de tareas de copia normal, copias de seguridad incrementales o diferenciales, pero no ambas.

Otro aspecto a tener en cuenta es la rotación de medios, un **esquema de rotación de medios** prevé cuántas cintas (u otro tipo de medios físicos) se utilizarán para realizar las copias de seguridad.

Un esquema de rotación popular se conoce como el **método del abuelo-padre-hijo** ya que utiliza tres "generaciones" de cintas que representan respectivamente copias de seguridad mensuales, semanales y diarias. En este esquema de rotación se realiza una copia de seguridad completa cada mes y se guarda la cinta durante un año (preferentemente en algún sitio seguro ajeno a la empresa); ésta es el "abuelo". Además se realiza una copia de seguridad completa semanalmente que se guarda durante un mes; ésta es el "padre". Las copias de seguridad que representan el "hijo" se realizan diariamente y se guardan durante una semana.

Independientemente del método que se utilice, la creación de un trabajo de copia de seguridad implica los siguientes pasos básicos:

1. **Seleccionar las unidades, directorios y archivos** de los que se quiera hacer una copia de seguridad.
2. **Especificar el medio de almacenamiento destino** de la copia de seguridad.
3. **Configurar las opciones de copia de seguridad** como tipo de copia de seguridad, registro y exclusión de archivos.
4. **Especificar cuándo se producirá** la copia de seguridad.

Para realizar una copia de seguridad de los archivos y carpetas, la cuenta utilizada para ejecutar la tarea debe tener los permisos de acceso apropiados para acceder a dichos archivos y carpetas.

Tan importante como realizar copia de los datos es hacer lo propio con la configuración de nuestro sistema, es decir los archivos de configuración como el registro y la base de datos de Active Directory. Realizar una copia de seguridad del estado del sistema es tan simple como seleccionar el cuadro apropiado en la pestaña de copia de seguridad, pero su restauración puede resultar un poco más complicada. El proceso de restauración no debe sólo sobrescribir los datos vitales del sistema actualmente en uso, como por ejemplo el registro, sino que debe también (en el caso de controladores de dominio) restaurar la base de datos Active Directory.

Para restaurar de forma efectiva el estado del sistema con un controlador de dominio, se deben realizar dos procedimientos especiales durante el proceso de restauración:

- iniciar el servidor en el modo de restauración de servicios de directorio
- y realizar una restauración autoritaria de la base de datos Active Directory.

Una **restauración autoritaria** es aquélla que indica los objetos restaurados del Active Directory como autoritarios, lo cual significa que durante el siguiente suceso de réplica, estos sobrescribirán los objetos equivalentes de los controladores de dominio que contienen las réplicas.

Microsoft y el mantenimiento del sistema.

Además de la gran cantidad de información impresa de la que disponemos en librerías especializadas. Internet proporciona la mayor fuente de información, en concreto Microsoft pone a disposición de los administradores y usuarios varios sitios dedicados a proporcionar nuevas técnicas, resolver dudas, etc. Uno de estos sitios es Microsoft TechNet,

14. Legislación Informática

La informática en la Constitución Española

Constitución Española, Título Primero. Capítulo II, Sección 1ª, Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Las leyes que serán objeto de estudio en esta unidad son las siguientes:

- Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 59/2003, de 19 de diciembre, de firma electrónica

Propiedad intelectual y programas de ordenador

TÍTULO VII. Del Real Decreto Legislativo 1/1996. PROGRAMAS DE ORDENADOR

Artículo 96. Objeto de la protección.

Resumen: *Es interesante comprobar que no sólo se protege a los programas sino que también están protegidas la documentación y los manuales. También es destacable que la protección se extiende a las versiones sucesivas. Muy interesante resulta destacar que no se pueden proteger mediante derechos de autor las ideas en las que se basan los programas.*

1. A los efectos de la presente Ley **se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas**, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.
2. A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. **La documentación técnica y los manuales de uso de un programa gozarán de la misma protección** que este Título dispensa a los programas de ordenador.
3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, **esta protección se extiende a cualesquiera versiones sucesivas** del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.
   Cuando los programas de ordenador formen parte de una patente o un modelo de

utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.

4. **No estarán protegidos** mediante los derechos de autor con arreglo a la presente Ley **las ideas** y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces.

Artículo 97. Titularidad de los derechos.

Resumen: *Los derechos son del creador o creadores, pero si la creación es hecha por un trabajador asalariado en el ejercicio de su trabajo la propiedad será de la empresa.*

1. **Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado**, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.
2. **Cuando un trabajador asalariado** cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como **el programa objeto, corresponderán, exclusivamente, al empresario**, salvo pacto en contrario.

El real decreo legislativo1/1996 (II)

Artículo 99. Contenido de los derechos de explotación.

Resumen: *El titular de los derechos de un programa debe autorizar la reproducción total o parcial, la traducción y la distribución pública, para que éstas sean legales.*

Los **derechos exclusivos de la explotación** de un programa de ordenador por parte de quien sea su titular con arreglo al artículo 97, incluirán el derecho de realizar o de autorizar:

1. **La reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria.** Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.
2. **La traducción, adaptación, arreglo** o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.
3. **Cualquier forma de distribución** pública incluido el alquiler del programa de ordenador original o de sus copias.

Artículo 100. Límites a los derechos de explotación.

Resumen: *Se autoriza la copia de seguridad por parte de quien tenga los derechos de explotación*

1. **No necesitarán autorización del titular, salvo disposición contractual en contrario, la reproducción o transformación de un programa de ordenador incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta.**
2. **La realización de una copia de seguridad por parte de quien tiene derecho a**

utilizar el programa no podrá impedirse por contrato en cuanto resulte necesaria para dicha utilización.

Artículo 102. Infracción de los derechos.

Resumen: *En este artículo se trata de forma específica el tema de la piratería, definiendo qué es.*

A efectos del presente Título y sin perjuicio de lo establecido en el artículo 100 tendrán la consideración de infractores de los derechos de autor quienes, sin autorización del titular de los mismos, realicen los actos previstos en el artículo 99 y en particular:

1. Quienes pongan en circulación una o más copias de un programa de ordenador conociendo o pudiendo presumir su naturaleza ilegítima.
2. Quienes tengan con fines comerciales una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima.
3. Quienes pongan en circulación o tengan con fines comerciales cualquier instrumento cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.

Artículo 103. Medidas de protección.

Resumen: *Complementario al artículo anterior, en éste se trata la protección legal de los derechos de autor.*

El titular de los derechos reconocidos en el presente Título podrá instar las acciones y procedimientos que, con carácter general, se disponen en el Título I, Libro III de la presente Ley y las medidas cautelares procedentes, conforme a lo dispuesto en la Ley de Enjuiciamiento Civil.

Se ve que la legislación española y las directivas europeas consideran los programas de ordenador como propiedad intelectual de la misma forma que las producciones literarias o musicales, y por lo tanto gozan de los mismos derechos y protección.

Propiedad Intelectual vs Patentes

El Parlamento Europeo en su sesión del 7 de julio de 2005 ha rechazado el cambio de propiedad intelectual a sistema de patentes, pero sigue siendo un tema controvertido que seguramente se reabrirá en el futuro. El cambio favorecería a las grandes empresas y multinacionales del sector y por lo tanto iría en detrimento de los pequeños desarrolladores y el usuario final que tendría que pagar el coste de las patentes.

Propiedad Intelectual y "piratería informática"

La "piratería informática" o copia y uso ilegal de programas, es una actividad antigua que empezó ha extenderse con la aparición de los primeros PC y la generalización del uso de la informática a nivel empresarial y doméstico, pero que ahora con el auge de las telecomunicaciones e Internet se ha incrementado enormemente, y preocupa a las empresas del sector. En 1988 se fundó la **BSA (Business Software Alliance)**, una asociación para luchar contra la piratería a nivel mundial.

El Código Penal español tipifica y establece las penas a los infractores de delitos contra la propiedad intelectual en sus artículos 270, 271 y 272.

Protección de Datos de Carácter Personal

Las principales normas que regulan la protección de datos de carácter personal son la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Ley Orgánica de Protección de Datos de Carácter Personal. LOPD.

La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre, establece una serie de obligaciones legales para aquellas personas físicas o jurídicas que posean ficheros con datos de carácter personal, en cuanto que estos contienen informaciones sensibles. En esta Ley también se crea la Agencia de Protección de Datos y se establecen su composición y funciones. Este organismo es el encargado de velar por el cumplimiento de la legislación en materia de protección de datos.

existe un Reglamento de Seguridad (Real Decreto 994/99, de 11 de junio) que desarrolla la mencionada Ley Orgánica y que establece la obligación de las empresas de cumplir una serie de medidas destinadas a garantizar la protección de dichos datos, afectando a los sistemas informáticos, los soportes de almacenamiento, el personal, los procedimientos operativos, etc.

Derechos de los ciudadanos sobre los datos de carácter personal

Esta Ley otorga a los ciudadanos varios derechos:

- **Impugnación de valoraciones:** Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
- **Derecho de consulta al Registro General de Protección de Datos:** Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.
- **Derecho de acceso:** Cualquier persona tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.
- **Derecho de rectificación y cancelación:** El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
- **Derecho de indemnización:** Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Las actuaciones que vulneran estos derechos pueden ser objetos de reclamación por los interesados ante la **Agencia de Protección de Datos.**

Obligaciones legales de la normativa de protección de datos

En la Ley Orgánica de Protección de Datos de Carácter Personal se establece la creación de un Registro General de Protección de Datos que será administrado por la Agencia de

Protección de Datos. En el Real Decreto 994/1999 se detalla el reglamento de seguridad para dichos ficheros. Se exige que el responsable del fichero elabore e implante la normativa de seguridad mediante un documento llamado **Documento de Seguridad**. En lo relativo a niveles de seguridad se establecen tres según sea la sensibilidad de los datos almacenados.

- **Nivel básico:** Ficheros que contengan datos de carácter personal.
- **Nivel medio:** Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).
- **Nivel alto:** Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. LSSI.

La norma más importante en este sentido es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Uno de los objetivos fundamentales de esta ley es la regulación del comercio electrónico, incorporando al ordenamiento jurídico español la Directiva Europea 200/31/CE que precisamente trata sobre el comercio electrónico.

Obligaciones de la LSSI

La LSSI regula las obligaciones de las empresas que utilicen Internet para realizar comercio electrónico, publicidad, o presten otros servicios. A continuación tienes un resumen de estas medidas.

Obligaciones de **empresas que utilicen Internet para realizar comercio electrónico**:

- En su página Web debe aparecer la siguiente información:
    1. Denominación social, NIF, domicilio y dirección de correo electrónico.
    2. Códigos de conducta a que estén adheridas.
    3. Precios de los productos o servicios que ofrecen.

- Deben comunicar el nombre de dominio de Internet que utilicen al Registro Mercantil u otro Registro público en que estén inscritas. Y si además efectúan contratos on-line deberán añadir la siguiente información:
    1. Trámites que deben seguirse para contratar.
    2. Condiciones generales a que, en su caso, se sujete el contrato.
    3. Confirmar la celebración del contrato por vía electrónica, mediante el envío de un acuse de recibo del pedido realizado.

Obligaciones de **empresas que hagan publicidad por vía electrónica**

- Identificar claramente al anunciante
- El mensaje debe resultar inequívocamente publicitario.
- Si se realizan ofertas, concursos o juegos promocionales, además de lo anterior, se deberá:
    1. Identificarlas como tales.
    2. Expresar de forma clara e inequívoca las condiciones de participación.
    3. Cuando se envíen por correo electrónico, mensajes SMS, etc., se obtendrá previamente el consentimiento del destinatario.

- Identificar el mensaje publicitario con la palabra «publicidad».
- Establecer procedimientos sencillos para facilitar la revocación del consentimiento por el usuario.

Para las **empresas que prestan otros servicios de la Sociedad de la Información** (Operadores de telecomunicaciones, proveedores de acceso a Internet (ISPs), prestadores de servicios de alojamiento de datos y buscadores)

- Colaborar con los órganos públicos para la ejecución de resoluciones que no puedan cumplirse sin su ayuda.
- Retener los datos de tráfico relativos a las comunicaciones electrónicas, de acuerdo con lo que establezca el Reglamento de desarrollo de la Ley.

Garantias de la LSSI

Como contrapartida a las obligaciones de las empresas, la LSSI garantiza ciertos derechos a los usuarios de servicios a través de Internet, a continuación se presentan los más significativos:

- Derecho a obtener información sobre los prestadores de servicios (nombre, domicilio, dirección de correo electrónico, etc.) y los precios de los productos o servicios que ofrecen.
- Respecto a la publicidad, derecho a conocer la identidad del anunciante, a no recibir mensajes promocionales no solicitados y a oponerse en cualquier momento a la recepción de los que hubieran autorizado.
- En la contratación, derecho a conocer los pasos necesarios para contratar por Internet, a acceder a las condiciones generales de la contratación antes de realizar su pedido y a obtener un acuse de recibo del vendedor que le asegure que su pedido ha llegado al vendedor.
- Si el consumidor realiza una compra a través de Internet, además se beneficia del régimen de protección que contempla la Ley de ordenación del comercio minorista para todas las ventas a distancia.

Administración electrónica y firma electrónica

Se conoce como administración electrónica la posibilidad de realizar trámites administrativos utilizando exclusivamente Internet como vehículo entre la Administración y el ciudadano.

Para que la administración electrónica sea un hecho se deben garantizar la confidencialidad e integridad de las comunicaciones entre ciudadanos, empresas, instituciones y administraciones públicas. Esto se regula por medio de la **Ley 59/2003, de 19 de diciembre**, de firma electrónica. En cuanto a los detalles técnicos y de implementación de la ley, la **FNMT (Fábrica Nacional de Moneda y Timbre)** ha puesto en marcha el proyecto **CERES (Certificación Española)**, que utiliza sistemas criptográficos.

Para poder interactuar con la administración a través de Internet, de manera que nuestra identidad sea reconocida sin lugar a error se utiliza el **certificado digital.** Este certificado se debe solicitar a la FNMT y debe ser instalado en un navegador de Internet, a partir de ese momento cuando se realicen trámites de forma telemática el usuario quedará identificado y a todos los efectos la gestión realizada tendrá la misma validez que si se hubiera hecho en persona. El certificado digital es la forma más extendida de firma digital.

Para solicitar y utilizar un certificado digital se deben realizar tres pasos:

- **Solicitar el certificado:** Conectando con la página Web de la FNMT, esta devolverá un código de solicitud con el que se deberá acudir a una Oficina de Acreditación.

- **Acreditarse en una oficina:** Dirigirse personalmente a una oficina registradora de cualquiera de los organismos que utilizan este tipo certificado para acreditar su identidad. Distintos organismos de la Junta de Andalucía proporcionan este servicio.
- **Descargar el certificado:** Se debe realizar una nueva conexión a la Web de la FNMT para descargar el certificado e instalarlo en el navegador.

El certificado digital **garantiza**:

- **Autentificación:** Identifica al usuario que ha enviado el mensaje.
- **Integridad:** Garantiza que no se ha alterado el mensaje.
- **No repudio:** Nadie excepto el emisor podría haber firmado el documento.