

Redes en educación 2

Capítulo 5

*Sistema operativos
de red*



ÍNDICE

1. Introducción.	5
1.1. ¿Qué es un sistema operativo?	5
1.2. Tipos de Sistemas Operativos.	6
a) Sistemas Operativos por su Estructura.	6
b) Sistemas Operativos por los servicios que ofrecen.	7
1.3. Sistemas operativos de red.	8
a) Sistemas operativos por la forma de ofrecer servicios.	9
b) Cliente/ Servidor y redes de igual a igual.	9
1.4. Sistemas operativos para equipos servidores.	11
1.5. Sistemas operativos para equipos cliente.	13
1.6. Elementos característicos de los sistemas operativos.	14
2. Redes Novell.	15
2.1. Características de las redes Novell.	15
a) Subsistema de almacenamiento de Netware.	15
b) Clientes y servidores de red.	16
c) Administración de directorios.	17
d) Administración de archivos.	18
e) Seguridad del sistema.	19
f) Administración de impresión.	19
2.2. Protocolo IPX/SPX.	20
a) Serie de protocolos Netware.	21
b) Protocolo IPX.	21
c) Protocolo SPX.	23
d) Protocolo principal de Netware (Netware Core Packet)	24
e) El Protocolo de Notificación de Servicios (SAP).	24
f) RIP. Protocolo de Información de Encaminamiento de IPX.	24
g) Configuración IPX sobre el router/bridge.	25
h) Encaminamiento IPX. Routers Novell.	25



Anotaciones

Capítulo 5

3. Redes de Microsoft Windows.	26
3.1. Características de las reedes Windows..	26
a) Gestión de discos.	26
b) Sistema de archivos.	27
3.2. Sistemas servidores de Windows.	29
a) Windows NT.	30
b) Windows 2000 Server.	35
c) Windows 2003 Server.	44
3.3. Sistemas clientes de Windows.	45
a) Windows 3.1	45
b) Windows 95	46
b) Windows 95	46
c) Windows 98	46
d) Windows Me (Millennium Edition)	48
e) Windows XP Professional.	49
3.4. Redes en Windows.	50
a) Componentes de la red Windows.	50
b) Instalación de una red con Windows.	50
c) Identificación del ordenador. Resolución de nombres.	51
d) Compartir conexión a Internet. Acceso telefónico a redes.	51
e) Conexión directa por cable.	51
f) Compartición de archivos.	52
g) Compartición de impresoras.	52
h) Administración remota.	52
i) Seguridad.	52
j) Monitor de red.	53
k) Conclusión.	54
3.5. Protocolos nativos de Windows.	55
a) Protocolo NETBIOS.	55

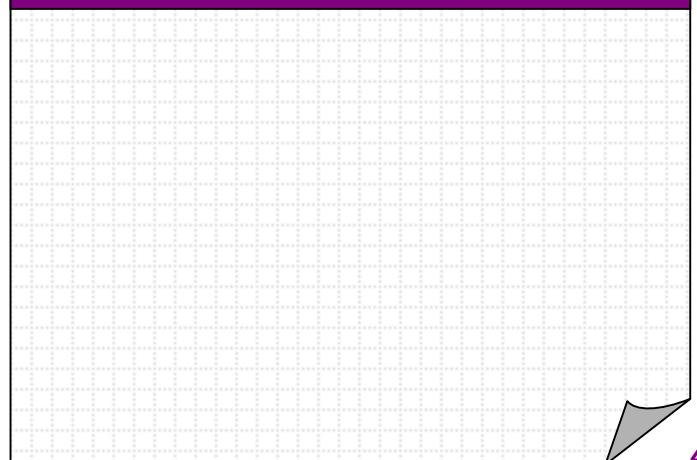
Anotaciones

Capítulo 5: Sistemas operativos de red

b) Protocolo NetBEUI.	57
c) Relaciones NetBIOS/ NetBEUI / TCP/IP	58
4. Redes Linux.	59
4.1. <i>Introducción.</i>	59
a) Breve historia de linux.	59
b) El concepto de software libre.	60
4.2. <i>Características del Sistema Operativo Linux.</i>	60
4.3. <i>Sistema de archivos de Linux.</i>	62
4.3. <i>Sistema de archivos de Linux.</i>	62
4.4. <i>Montaje de dispositivos.</i>	64
4.4. <i>Montaje de dispositivos.</i>	64
4.5. <i>Aspectos generales.</i>	65
4.5. <i>Aspectos generales.</i>	65
a) Intérpretes de comandos “shell”.	65
b) Entorno gráfico.	65
c) Usuarios y grupos.	66
4.6. <i>Administración.</i>	69
a) Sistemas de permisos. Administración de archivos.	69
b) Compartición de recursos.	70
c) Sistema de directorios.	72
d) Seguridad del Sistema.	73
4.7. <i>Protocolos de comunicación en redes con Linux.</i>	74
a) UUCP.	74
b) TCP/IP.	74
5. Otros sistemas operativos.	75
5.1. <i>Microsoft LAN Manager.</i>	75
5.2. <i>IBM LAN Server.</i>	76
5.3. <i>Redes Apple.</i>	76
Ilustraciones	77

Anotaciones

Anotaciones

A large rectangular area filled with a light gray dotted grid, intended for handwritten notes. In the bottom right corner of the grid, there is a small, dark gray triangular shape.

1. Introducción.

Ya hemos comentado que una red es un conjunto de equipos informáticos interconectados entre sí. Supongamos que tenemos los equipos, el cableado, las tarjetas de red y sus controladores y un planteamiento general del tipo de red que vamos a utilizar. Pero algo no se nos debe escapar, antes de comenzar a instalar la red debemos pensar en el tipo de *sistema operativo de red* que más nos conviene utilizar en función de las tareas que queremos que desempeñe nuestra y los recursos de los que dispongamos.

Nota:

Sin un sistema operativo de red, ya sea servidor o estación de trabajo, un equipo no puede conectarse a una red, pues una de las funciones que realiza un sistema operativo es la gestión de esta conexión. Actualmente, la mayoría de los sistemas operativos existentes en el mercado, por no decir la totalidad, soportan en mayor o menor medida el trabajo en red.

En este tema comentaremos de manera breve los distintos sistemas operativos de red que podemos utilizar, así como sus características fundamentales.

Para pensar:

¿Recuerdas la versión 3.11 de Windows, podrías decir si esta versión permitía el trabajo en grupo?

1.1. ¿Qué es un sistema operativo?

Como sabemos, una computadora está formada de dos componentes fundamentales: hardware y software. El sistema operativo es la parte esencial de este último. Si nos imaginamos la estructura de nuestra máquina como una pirámide, en la base tendríamos el hardware: las unidades de disco, la memoria disponible, el procesador, los dispositivos periféricos como son las impresoras o faxes..., y superpuesto parcialmente con el hardware tenemos nuestro *Sistema Operativo*, con programas especializados llamados controladores de dispositivo que permiten que el sistema operativo imparta órdenes al hardware.

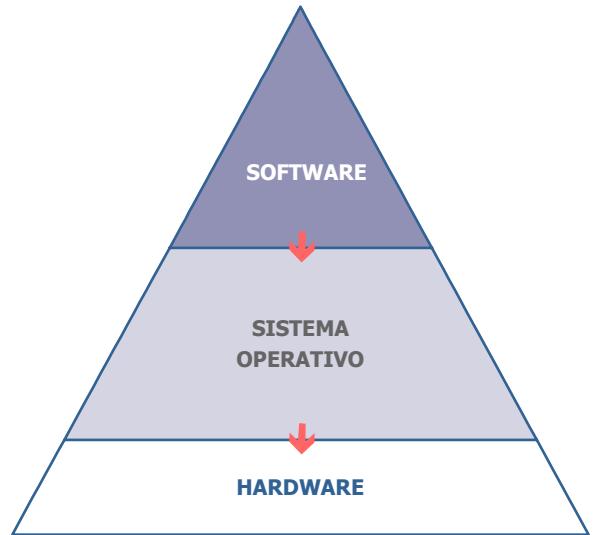


Ilustración 1: El S.O. es el software que ejerce de intermediario entre el resto de las aplicaciones y el hardware

Anotaciones

Capítulo 5

El Sistema Operativo se trata pues, de un software básico que actúa como intermediario entre el usuario y el hardware de un ordenador, controlando y administrando los recursos de la computadora de manera más sencilla, cómoda y eficiente. Estos recursos son:

- Memoria.
- Tiempo de CPU.
- Espacio de disco.
- Periféricos.

Actualmente, los sistemas operativos presentan estructuras que permiten realizar estas operaciones con mayor flexibilidad e independencia del hardware sobre el que se montan.

1.2. Tipos de Sistemas Operativos.

Los sistemas operativos se han clasificado tradicionalmente siguiendo estos criterios:

- Por su estructura.
- Por los servicios que ofrecen.

a) Sistemas Operativos por su Estructura.

Según esta clasificación, los sistemas operativos pueden poseer las siguientes estructuras.

- Estructura monolítica o modular
- Estructura jerárquica o por capas

En la estructura monolítica o modular el sistema se dispone como un conjunto de procedimientos entrelazados de tal forma que cada uno puede llamar a cualquier otro. Un ejemplo de Sistema Operativo monolítico típico es Unix. Son sistemas en las que la interdependencia entre sus elementos es total, no pueden trabajar unos sin los otros.

La estructura jerárquica consiste en organizar el sistema como una jerarquía de capas que podemos ver de varias formas:

- Como un sistema operativo en niveles, cada uno sobre el inmediatamente inferior. El primer sistema construido de esta manera fue el sistema THE (Technische Hogeschool Eindhoven).
- Como un sistema organizado en anillos, presentado en el sistema MULTICS.

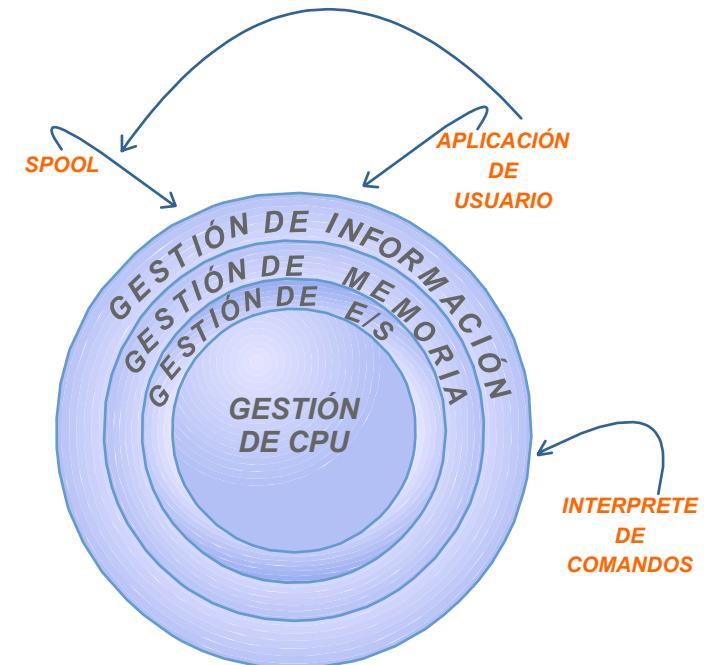


Ilustración 2: Sistema operativo de estructura jerárquica en anillos concéntricos.

Anotaciones

En este sistema, las zonas más internas o núcleo están más protegidas de posibles accesos indeseados desde las capas más externas y tienen un contacto más próximo con el hardware.

Los sistemas operativos modernos tratan de mover el código a capas superiores y así conseguir un sistema operativo con núcleo mínimo, más seguro y ágil.

Nota:

Un usuario solicita un servicio, como la lectura de un archivo de texto. Entonces un proceso del usuario (proceso cliente) envía la solicitud a un proceso servidor, que se encarga de realizar el trabajo, ejecutando el procesador de texto. El núcleo simplemente controla la comunicación entre cliente y servidor.

Podríamos decir que el sistema esta dividido en pequeñas partes que controlan distintas funciones, como el servicio a archivos o servicio a la memoria. De esta manera si hay un error en cualquiera de los procesos servidores, éstos pueden fallar, pero sin afectar a todo el sistema. De esta forma trabajan los sistemas operativos “Microkernel” o de procesos “cliente / servidor”.

b) Sistemas Operativos por los servicios que ofrecen.

Siempre hemos escuchado los términos *monotarea* o *monousuario*. Es evidente que los sistemas operativos monousuarios soportan un solo usuario a la vez, caso típico de los primeros ordenadores personales o PCs.

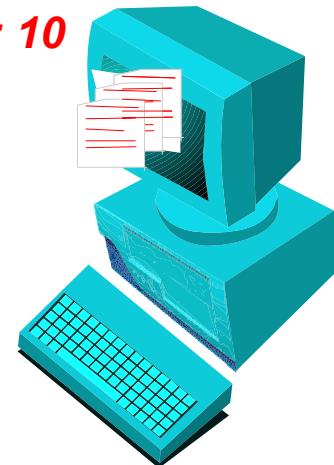
Los Sistemas operativos monotarea son primitivos y sólo manejaban una tarea a la vez por usuario, es decir, ejecutaban las tareas de una en una. Claro ejemplo de estos dos casos es MS-DOS, siglas de Microsoft Disk Operating System (sistema operativo de disco de Microsoft), sistema operativo monotarea y monousuario que trabajaba con una interfaz de línea de comandos.

Los sistemas operativos actuales suelen ser *multiproceso*, *multitarea* y *multiusuario*. Procesan varias labores al mismo tiempo y son capaces de dar servicio a más de un usuario a la vez. Normalmente ejecutará tantas tareas como procesadores tenga, y si el número de tareas es superior al número de procesadores, el equipo distribuye la carga de trabajo entre ellos, dedicando ciertas cantidades de tiempo a cada tarea en función de unos criterios de prioridad.

00: 01



00: 10



00: 05



Ilustración 3: Un sistema operativo multitarea puede ejecutar varias tareas a la vez dedicando un tiempo a cada una de ellas en función de su prioridad.

Anotaciones

1.3. Sistemas operativos de red.

Las clasificaciones que hemos analizado hasta ahora, nos han posibilitado conocer las características básicas de cualquier sistema operativo. Ahora bien, con relación al tema que estamos trabajando, deberemos realizar una nueva clasificación:

- Sistemas operativos para equipos autónomos. Se trata de los sistemas operativos que se instalaban en las primeras máquinas y cuya función era la del control y gestión eficiente del software y el hardware de cada equipo, no se contemplaba su interconexión.
- Sistemas operativos para equipos conectados a una red. Sistemas que se han desarrollado a partir de las posibilidades de comunicación entre máquinas y que se pueden subdividir en:
 - Sistemas operativos para equipos servidores.
 - Sistemas operativos para equipos clientes.

Así, un sistema operativo para equipos conectados a una red debe realizar las funciones descritas hasta ahora y, además:

- Permitir, gestionar y coordinar la conexión y funciones de todos los elementos que integren la red (equipos y periféricos).
- Facilitar la seguridad de todos los recursos que estén integrados en la red.

Si quisieramos que un equipo autónomo se incorporara a una red informática deberíamos modificar su sistema operativo integrando las funciones necesarias o instalándole otro que permitiera su conexión y funcionamiento en red.

Nota:

Cuando disponemos de un ordenador con un sistema operativo que no ha estado conectado a una red, al instalarle el adaptador de red observamos que no llega a ver al resto de los equipos o que no puede acceder a la red, esto es debido a que no se le han instalado los servicios del sistema operativo que van a permitir su incorporación a la red.

En cualquier caso, esta clasificación también puede ser matizada en la forma en que deseemos que se ofrezcan los servicios y desde el tipo de red que deseemos implementar.

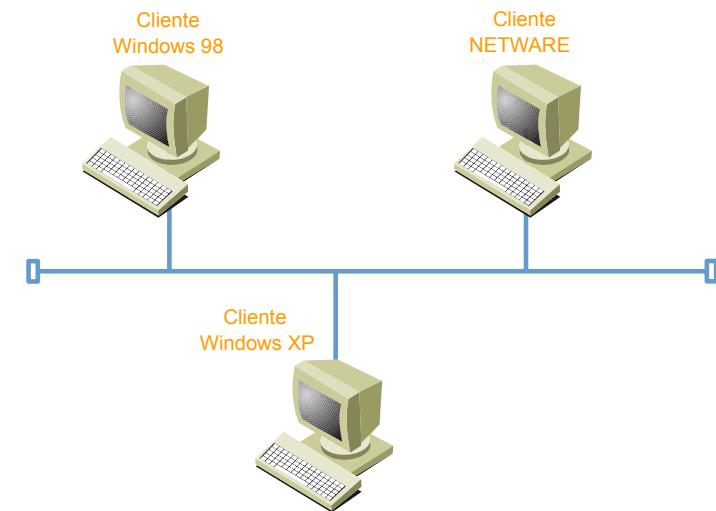


Ilustración 4: Para que un equipo se pueda conectar a una red requiere de la instalación de un S.O. que admita una de las opciones de cliente o servidor de red.

Anotaciones

a) Sistemas operativos por la forma de ofrecer servicios.

Si miramos desde el punto de vista del usuario, apreciamos varias formas de acceder a los servicios. Así, nos encontramos con dos tipos principales: sistemas operativos de red y sistemas operativos distribuidos.

Sistemas operativos de red.

También conocido como NOS (Network operative system). Realmente se trata de un software que es necesario para integrar los componentes de la red, como archivos, periféricos y recursos, en un todo al cual el usuario final tiene un cómodo acceso. El sistema operativo de red controla y administra todos estos recursos, así el usuario se libra de posibles conflictos en el momento de usar la red.

Un equipo no puede trabajar sin sistema operativo, pero a su vez, una red de equipos es inútil sin un sistema operativo de red. De esta manera el usuario puede ver otros equipos conectados en red con sus sistemas operativos y usuarios o grupos de usuarios locales. Puede comunicarse con ellos e intercambiar información, ejecutar tareas, transferir archivos, etc. Es esto último la principal función de un sistema operativo de red, pero para ello el usuario debe copiar explícitamente el archivo de una instalación a otra, o sea, debe conocer el nombre del archivo y saber qué se ubica en éste o aquel equipo.

Sistemas operativos distribuidos.

El usuario percibe al sistema como un ente simple formado por un único procesador, aunque sean varios procesadores los que formen el sistema. El usuario trabaja sobre una máquina virtual sin saber en que equipo está este o aquel fichero. Para él, todo está en local y forma un sistema operativo único.

Aunque se han realizado grandes esfuerzos no se ha conseguido crear un sistema distribuido completo del todo, por la complejidad que suponen. El simple hecho de distribuir los procesos en las varias unidades de procesamiento, o de agrupar los resultados, así como resolver fallos o consolidar la seguridad entre los diferentes componentes del sistema, es una tarea enorme. Entre los diferentes sistemas operativos distribuidos que existen tenemos: Solaris, Mach, Chorus, NIS, Taos, etc.

b) Cliente/ Servidor y redes de igual a igual.

De todos es conocido el concepto Cliente/ Servidor, donde es necesario que una computadora trabaje como servidor, proporcionando servicios que son demandados por los equipos clientes. El sistema operativo Novell Netware es un ejemplo de este caso.

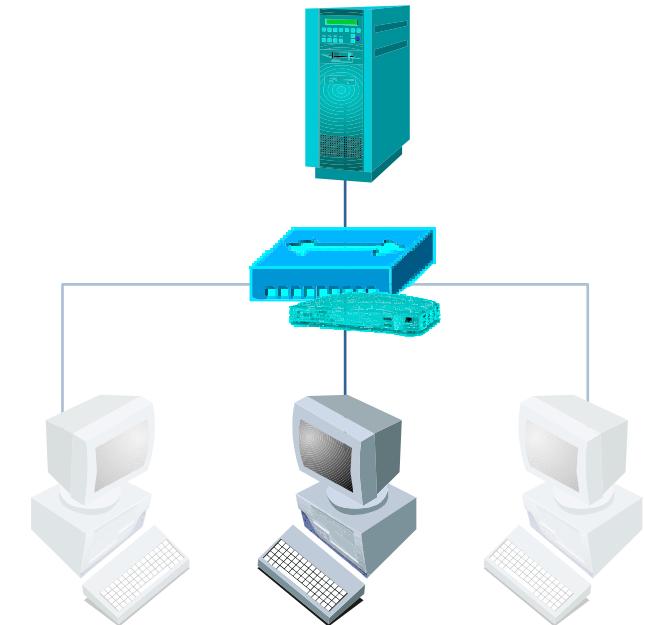


Ilustración 5: En un S.O. Cliente-Servidor puro, una estación de trabajo no puede "ver" al resto, sólo puede acceder al servidor

Anotaciones

Capítulo 5

En oposición, una red “entre iguales” posee equipos que pueden funcionar tanto en forma de cliente como en servidor. Windows 2000 tiene las dos versiones: Professional y Server, pero se trata de un sistema operativo de red entre iguales, puesto que cualquier equipo con Windows 2000 puede compartir sus recursos con otro 2000, sin importar si es un Server o Professional. Los equipos cliente en una red Novell Netware no pueden actuar como servidores para otros equipos clientes, esta tarea sólo puede ser ejecutada por un ordenador cuyo sistema operativo sea de servidor.

Nota:

Es importante no confundir los conceptos de red cliente-servidor, con los de servidor y cliente de una petición y con el de software de sistema operativo de servidor y de cliente. Una red Novell cliente-servidor no permite las peticiones entre equipos, una red Windows con un Windows 2000 Server permite este tipo de peticiones pero, a la vez, existe un ordenador servidor que puede gestionar y controlar el acceso a la red atendiendo peticiones de servicios o incluso solicitando él mismo dichos servicios.

Dependiendo del fabricante del sistema operativo, el software de red está incluido en el propio sistema o es necesario añadirlo. En el segundo caso tenemos los sistemas Novell Netware. El equipo necesita ambos sistemas operativos: para procesar el trabajo en red y para gestionar sus propias funciones.

El software del sistema operativo de red se integra en casos como Windows NT Server/ Windows NT Workstation, Windows 2000 Server, Windows 2000 Professional, Windows Me y XP entre otros. En estos casos, y aunque existan los roles de cliente y servidor, se tratan de sistemas operativos entre iguales.

Analogía:

Un sistema cliente/servidor puro sólo permite la comunicación con el servidor como intermediario. El servidor es como un jefe que todo lo controla y no permite el intercambio de ideas entre empleado. Sin embargo, un servidor en una red entre iguales se encarga de coordinar, permite el trabajo entre iguales y lo que hace es garantizar que esta comunicación sea de la mejor calidad.

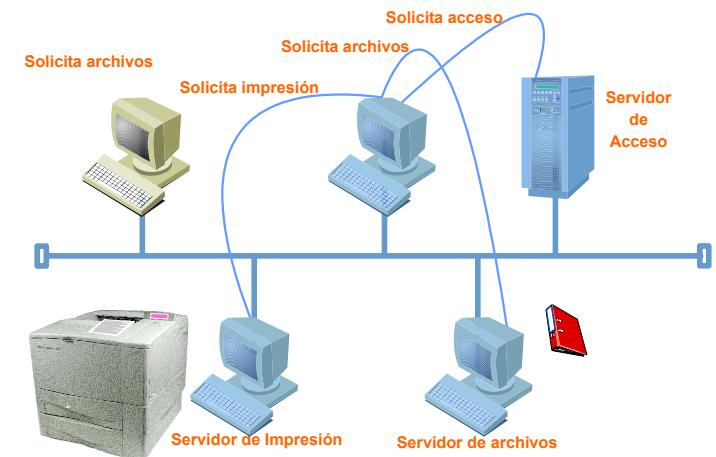


Ilustración 6: En una red de igual a igual con servidor, existe un equipo que se encarga de gestionar el acceso a la red y sus recursos, aunque no es, necesariamente, el único equipo que proporciona servicios a la red.

Anotaciones

1.4. Sistemas operativos para equipos servidores.

Los entornos de sistemas operativos de red más comunes son tres:

- Novell Netware.
- Microsoft Windows.
- UNIX/ Linux.

La mayor diferencia entre estos sistemas es que, desde sus comienzos, Novell Netware ha sido un sistema cliente/servidor puro, mientras que Unix y Windows han desarrollado redes en las que cualquier estación de trabajo podía actuar como cliente o servidor de ciertas aplicaciones, con independencia de la existencia de un equipo con un sistema operativo servidor instalado.

Nota:

Existen varias distribuciones distintas de software basado en UNIX y Linux, desarrolladas por distintas empresas.

Un software servidor debe permitir:

- Compartir recursos: El sistema operativo debe encargarse de poner los recursos a disposición del resto de los equipos, especificar determinar el control y acceso que pueden realizar los distintos usuarios de dichos recursos y, por último, coordinar el acceso a los mismos.
- Gestionar los usuarios de manera que se determine qué usuarios pueden acceder a la red y en qué situación.
- Administrar y controlar el estado de la red.

Un equipo servidor, tal como ya hemos indicado, es aquel que presta una serie de servicios a otros equipos. Si tenemos en cuenta la posibilidad que un entorno de red (Novell, Windows o Unix/Linux) ofrece para la presencia de equipos que actúen como servidores, podríamos crear una gradación de situaciones en cuanto a la flexibilidad que proporciona cada uno de los sistemas operativos.

Nota:

Debemos desligar el concepto de servidor del de PC, puesto que un servidor puede ser un router que asigne direcciones IP de forma dinámica. Un servidor es cualquier dispositivo que presta un servicio en una red de ordenadores.



Ilustración 7: Un servidor gestiona el acceso a la red por parte de los usuarios

Anotaciones

Capítulo 5

En las redes Novell es únicamente, el equipo servidor, con la aplicación de servidor instalada, el que puede realizar estas funciones. Los equipos con aplicaciones clientes no pueden encargarse de ninguna de estas tareas.

En las redes Windows, equipos con sistemas operativos cliente, pueden ser habilitados para ofrecer servicios (actuar como servidor) al resto de los equipos de la red, sin embargo, sólo los sistemas operativos de servidor Windows NT Server o Windows 2000 Professional Server pueden gestionar el acceso a la red. De este modo, en una red sin servidor Windows y con estaciones cliente de este sistema operativo, cada usuario controlaría el acceso a su equipo, sin la posibilidad de crear un control centralizado.

Por último, las redes Linux son completamente flexibles, en cualquier equipo, con independencia de la distribución que posea, puede actuar como servidor e implementar cualquier servicio, no hay ningún tipo de restricciones en este sentido.

Las situaciones que acabamos de plantear parten de la idea de redes con sistemas operativos homogéneos, sin embargo, actualmente, una red informática puede estar constituida por ordenadores que monten sistemas operativos distintos y será el sistema operativo servidor el que condicione el comportamiento de dicha red. Para ello se han habilitado, desde las distintas empresas aplicaciones que se pueden instalar tanto en clientes como en servidores que posibilitan esta interoperatividad de sistemas.

En cualquier caso, con independencia del sistema operativo que utilicen, deben comunicarse entre sí con un lenguaje común, es decir, debemos habilitar en todos ellos el mismo protocolo de comunicaciones ya sea NetBEUI, TCP/IP, IPX/SPX, etc. pues, en caso contrario, los equipos no podrían comunicarse entre sí.

Nota:

Para conectar un equipo con Windows 98, por ejemplo, a una red Novell se requiere la instalación de la pila de protocolos IPX/SPX y el servicio de cliente para Netware.

Para pensar:

¿Qué sucedería si en una misma red tuviéramos un servidor de DHCP de Linux y otro de Windows?, ¿pasaría lo mismo si se trataran de servidores de FTP?, ¿por qué?

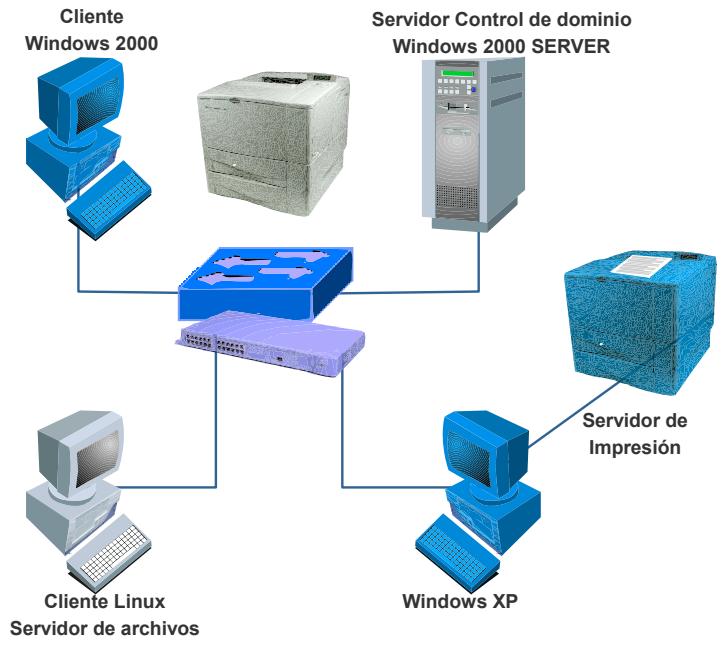


Ilustración 8: Actualmente existe una alta interoperabilidad entre sistemas operativos para el trabajo en red.

Anotaciones

1.5. Sistemas operativos para equipos cliente.

Cuando trabajamos con un ordenador autónomo, todas las peticiones de servicios se realizan dentro del equipo, sin embargo, en un ordenador conectado a una red se requiere de un sistema que permita cursar órdenes y peticiones al exterior. El equipo ya no cursa órdenes a un único procesador, sino que lo puede realizar a todos aquellos que se encuentren en la red.

El sistema operativo debe emplear una aplicación (“shell”) que se encargue de controlar las peticiones que realiza el equipo identificado como cliente y redirigirlas al equipo que dispone de dicho recurso dentro de la red de redirigir las peticiones. Estas aplicaciones son conocidas como **redireccionadores** y son distintas en función del tipo de red en el que nos encontramos.

Además, estas aplicaciones, puede crear referencias de elementos externos al PC asignándole objetos internos. Por ejemplo, una carpeta compartida de un PC en la red puede recibir la asignación de una letra de unidad de red, o la petición de impresión a un puerto del equipo puede ser dirigida a una impresora compartida por otro equipo.

Analogía:

Un redirector es similar a una persona que se encargara de crear analogías como esta dentro del PC, si realizo una petición de un archivo externo el redirector le dice “bueno, pues lo hacemos a tu unidad G:” cuando en realidad esa unidad física no existe dentro del equipo . Es decir, simplifica todo el trabajo a la hora de realizar las peticiones de servicios creando referencias internas a elementos externos. Engaña al PC para que piense que se encuentra solo cuando en realidad actúa dentro de una red.

Los distintos sistemas operativos condicionan la forma en la que van a actuar los clientes dentro de la red. Así, en Windows, necesitamos instalar el servicio de “compartir archivos e impresoras” para que nuestro equipo cliente actúe como servidor y cliente de archivos y periféricos, mientras que en Linux, deberemos instalar un servidor Samba para compartir archivos en una red con equipos Windows o puntos de montaje NFS con equipos Linux. Sin embargo, con independencia del S.O. del que se trate, un software cliente debe posibilitar que esa máquina pueda acceder a archivos remotos, elementos de hardware de otros equipos, además de posibilitar la identificación, bien en la máquina local, bien en un servidor remoto, del usuario que accede en ese momento al equipo y, por lo tanto, a la red de ordenadores.

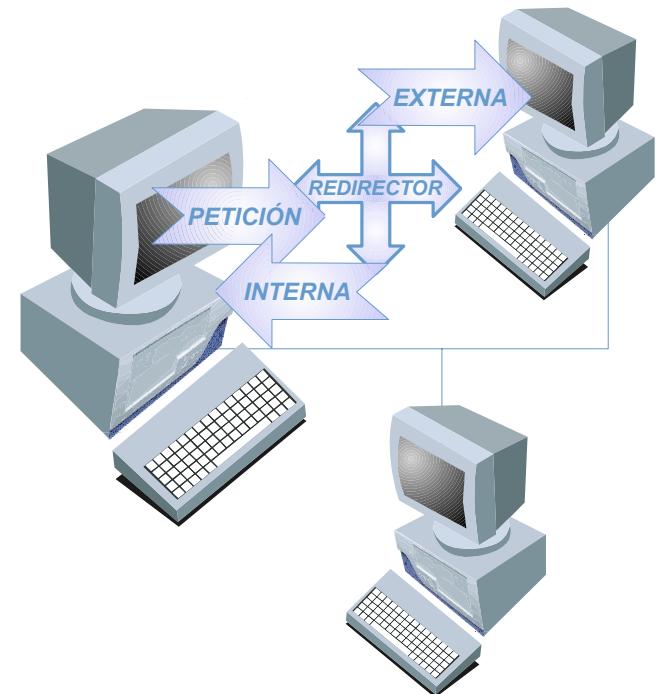


Ilustración 9: El redirector es la aplicación que hace transparente el uso de la red, gestionando y redirigiendo las peticiones de servicio.

Anotaciones

1.6. Elementos característicos de los sistemas operativos.

Además de por su arquitectura, Los distintos sistemas operativos se diferencian por las soluciones que aportan a los requisitos de funcionamiento de un PC y de una red. Tal como hemos indicado, el sistema operativo se encarga de enlazar las aplicaciones con los dispositivos de hardware, por lo que deberá controlar elementos de ambas subestructuras.

- Sistemas de archivos. La forma de almacenar y localizar los ficheros en un disco duro es uno de los primeros problemas a resolver. Cada sistema operativo aporta una solución; así, Novell emplea el sistema DET o Windows 2000 NTFS. Además, cada sistema de almacenamiento supone la toma de decisiones sobre cómo se van a particionar las unidades de disco y cuáles van a ser los tamaños de las unidades mínimas de almacenamiento.
- Servicios de directorio. Base de datos centralizada de los recursos de la red. Cuando, en un principio existía un único servidor, y las redes no tenían un gran tamaño, la ubicación de los distintos objetos de la red y su administración era sencilla. Sin embargo, según fueron creciendo las redes y aumentando el número de servidores este problema se agravó. Era necesario crear una base de datos que recogiera y centralizara toda la información. Los servicios de directorio como el NDS de Novell o el Active Directory de Windows son dos soluciones distintas a este mismo problema.
- Seguridad de los servicios. Otra tarea de los sistemas operativos es proporcionar seguridad para, por un lado administrar los servicios de directorio y, por otro para el servicio propiamente dicho. En muchos casos conviene que la base de datos esté repartida por varios servidores (aunque disponga de un único acceso), esta distribución permite que los datos almacenados se encuentren próximos a los elementos a los que hacen referencia, sin embargo, al estar la Base de datos repartida, es necesario establecer estrategias que coordinen las actualizaciones de datos, los accesos y las copias de seguridad.
- Organización de la red. Los distintos objetos que configuran una red se pueden agrupar en dominios o grupos de trabajo. La principal diferencia entre ambos es que el control de acceso sea centralizado o local. Los sistemas operativos pueden implementar una o ambas de estas estructuras posibilitando así la creación de distintos tipos de redes.
- Protocolos de comunicación. Protocolos nativos que emplean los sistemas operativos para la comunicación en la red.

Cuando procedamos a analizar cada uno de los sistemas operativos, centraremos nuestro estudio en estos aspectos.

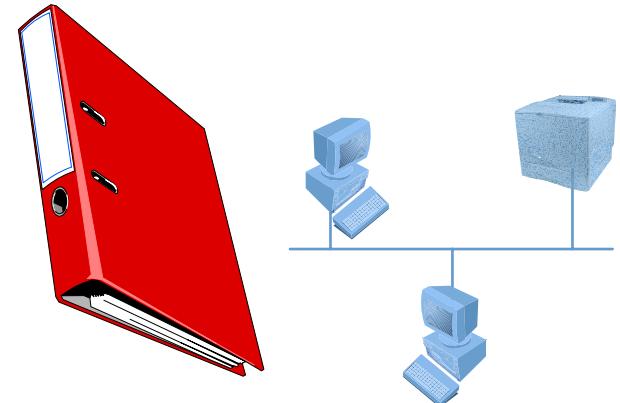


Ilustración 10: Servicio de Directorio: Es una base de datos centralizada en la que se recogen todos los recursos disponibles en una red

Anotaciones

2. Redes Novell.

2.1. Características de las redes Novell.

Netware es un sistema operativo diseñado por Novell Data System a finales de la década de los 70 a partir de UNIX y CP/M. En principio gestionaba terminales no inteligentes que se conectaban a un equipo servidor donde se realizaban todas las operaciones. Sus principales aportaciones fueron la utilización de un servidor de archivos en lugar de un servidor de discos, la utilización de un PC IBM y la independencia del tipo de hardware sobre el que se instalara el sistema operativo.

Una red Novell se compone de un equipo servidor con el sistema operativo Novell NetWare instalado y una serie de estaciones de trabajo con distintos sistemas operativos (Windows, Linux, etc.) y sobre los que se instala una aplicación de Novell para que se pueda acceder al servidor de red Netware.

Las redes Novell permiten una gran flexibilidad a la hora de su configuración, así NetWare 5.1 puede soportar redes conectadas por módems con miles de equipos, así como ordenadores mainframe hasta mini ordenadores, múltiples servidores de archivos, etc.; siendo a la vez capaz de funcionar en cualquier topología.

A pesar de su gran eficacia, las redes Novell se encuentran en desventaja con respecto a otros tipos de redes, sin embargo, se debe más a un error en las políticas de implantación y promoción que a su calidad.

a) Subsistema de almacenamiento de Netware.

El sistema de archivos de Novell es un sistema propietario, aunque pueda coexistir con otros sistemas como FAT o NTFS. Este sistema consta de particiones (una por unidad de disco duro) y volúmenes, elementos en los que se fragmenta una partición. Al igual que los clusters en una partición FAT, Novell emplea bloques de asignación de discos a los que se les puede dar un tamaño variable en función del tipo de archivos que se van a guardar en ese volumen. Si se desean guardar archivos de gran tamaño se puede usar bloques de 64 kb, mientras que si los archivos son más pequeños se pueden emplear bloques de 4 kb. Sin embargo, los bloques de mayor tamaño permiten un mejor aprovechamiento del disco, puesto que el acceso a la información es más rápido.

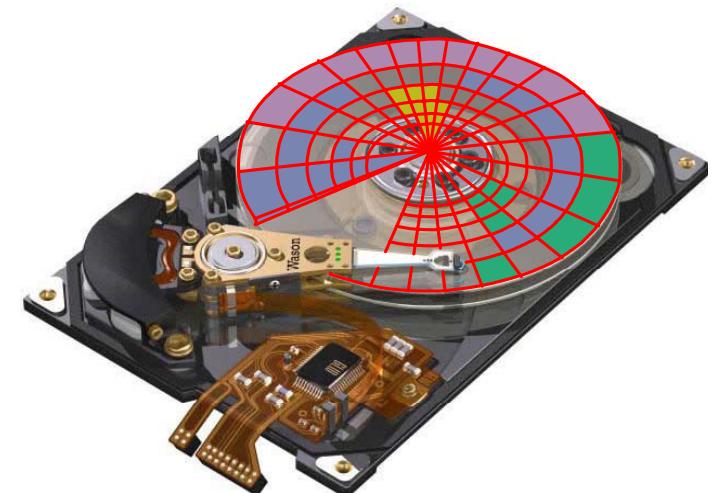


Ilustración 11: Sistema de archivos

Anotaciones

Cada volumen dispone de una tabla de entradas de directorio donde se almacenan la información de los archivos que contiene ese volumen, de manera que cada archivo o cada directorio que estén dentro de ese volumen tienen una referencia en el DET.

Nota:

Las tablas FAT en Novell son usadas para indicar en qué bloques de un volumen se encuentra un archivo. Mientras que emplea DET para recoger la información de archivos y directorios que no requiere un acceso a ellos.

Aunque en principio Novell no admite nombres de archivos de más de ocho caracteres mediante el Espacio de nombres se pueden crear enlaces entre los archivos originales y nombres de hasta 256 caracteres, aunque aumenta el número de entradas que se incorporan a la DET y ralentiza el acceso a los archivos.

La idea fundamental de este sistema de archivos es alcanzar un uso óptimo de los discos en el servidor, para así prestar un mejor servicio a los clientes.

b) Clientes y servidores de red.

El sistema operativo Novell está orientado para que todos los recursos compartidos se almacenen en servidores, de manera que en las estaciones clientes no se encuentre ningún recurso compartido. Se trata de un sistema de red cliente-servidor puro en el que pueden coexistir varios servidores.

El sistema de archivos que acabamos de explicar se fundamenta en esta idea, es decir, el servidor debe dar el servicio más rápido a los clientes a través de un S.O. y un subsistema de archivos diseñado para ello, mientras que las estaciones clientes no deben necesitar un S.O. específico, sino un protocolo de comunicación que facilite el acceso al servidor.

En una red Novell el servidor es el encargado de correr el sistema operativo y de controlar los datos que circulan por la red, es el centro neurálgico de la red, incorporando en las últimas versiones el servicio de acceso a Internet. Las estaciones cliente disponen de su propio sistema operativo y de una aplicación para Novell que permite su comunicación, creando la sensación a los usuarios de que aún cuando los archivos se encuentren en el servidor, se están ejecutando en su propia máquina.

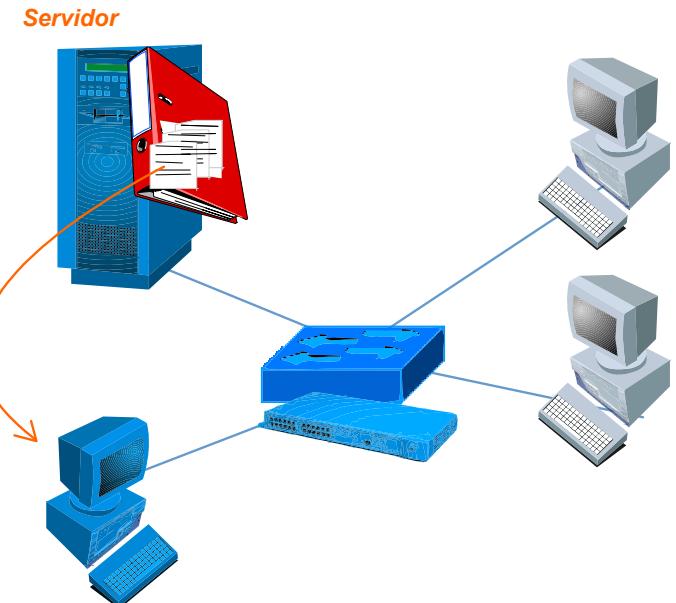


Ilustración 12: En una red Novell los únicos equipos que pueden compartir archivos son los servidores

Anotaciones

c) Administración de directorios.

Cada usuario que es registrado en la red dispone de un subdirectorio privado en un servidor, donde el usuario guardará todos sus datos e información. El usuario dispone de un control total de su directorio y tiene la facilidad de que el administrador de red gestiona sus copias de seguridad al encontrarse en el servidor.

Los directorios son interpretados como unidades de red de manera que, como cada estación soporta hasta veintiséis unidades de red, un usuario puede moverse entre estas unidades al igual que se mueve por las unidades de disco de su equipo.

Esta situación era bastante sencilla de administrar cuando existía un único servidor, sin embargo, cuando una misma red disponía de múltiples servidores era necesario registrar a cada usuario en cada uno de ellos. Era conveniente establecer un sistema que facilitara la administración de todos los recursos y usuarios. A partir de la versión 4 de Netware se solucionó este problema con el servicio de directorios de Novell que actualmente es un modelo imitado por el resto de sistemas.

NDS (Novell Directory Services).

Se trata de una base de datos relacional en la que participan todos los servidores de la red, que recoge todos los objetos que se encuentran en la ella (por grande que sea y el número de servidores de que disponga) y que permite presentar tanto a los usuarios como al administrador en un modo gráfico, todos los recursos disponibles en la red, bien para su acceso, bien para su administración, en función de los permisos que se posean. Se trata de una aplicación que facilita el control y el acceso a todos los recursos de la red.

Esta base de datos se compone de objetos que pueden representar usuarios, elementos de hardware, software, etc. y que adoptan una estructura de árbol jerárquica.

Nota:

NDS puede funcionar sobre Novell Netware, Windows o Linux proporcionando idénticos servicios.

Los objetos pueden ser de dos tipos:

- Contenedores: objeto con otros objetos subordinados.
- Hojas: Objeto que no puede tener otros dentro.

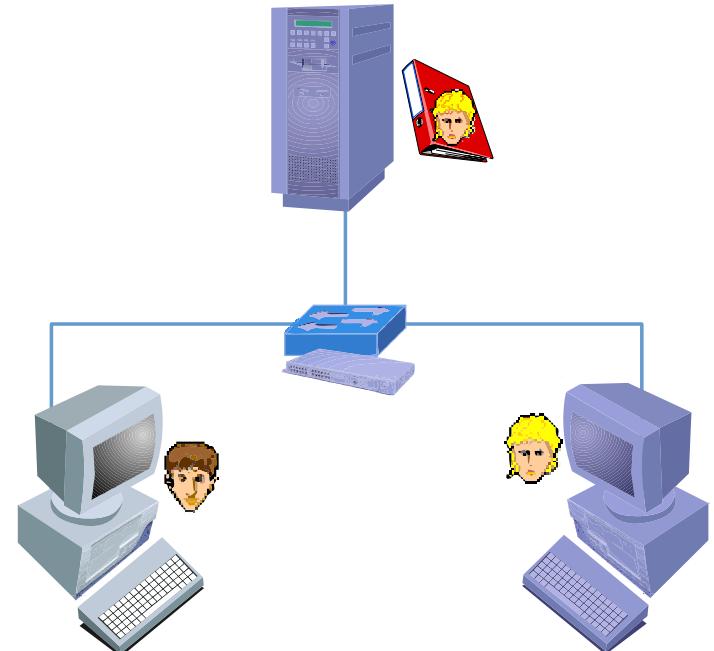


Ilustración 13: Login y acceso a un directorio del servidor: cada usuario dispone de un subdirectorio privado al que accede una vez que se ha identificado

Anotaciones

Un objeto contenedor sería un elemento basado en una premisa organizativa mientras que las hojas serían servidores, usuarios, etc. clasificados en función del criterio que ha generado los contenedores. Pueden existir objetos con el mismo nombre siempre y cuando no se encuentren en el mismo contenedor ya que NDS utiliza la ruta de su ubicación dentro del árbol para identificar el objeto.

Analogía:

Si quisieramos identificar a todos los ciudadanos que viven en España de una forma eficiente podríamos crear un árbol cuyas primeras ramas fueran los distritos postales, el segundo nivel, las calles de ese distrito, el tercer nivel los portales, el cuarto las escaleras, el quinto los pisos, el sexto las puertas, el séptimo los apellidos y el octavo el nombre. Pero ese objeto, nombre podría tener hojas que fueran la edad, el sexo, etc.

Ahora bien, este sistema no es necesariamente el único, puesto que podríamos crear otro que se iniciara por el sexo, la edad, etc. Así, un mismo centro gestionado por dos administradores, podría tener dos estructuras jerárquicas distintas.

NDS es, como ya hemos dicho, una base de datos. Al disponer la red de múltiples servidores, estos deben acceder a esta base de datos de forma constante, por lo que es recomendable que no se encuentre alojada en un único servidor sino que se reparta por toda la red, siendo cada una de las partes de la base de datos una de las ramas del árbol y alojando esa partición en aquel servidor que más requiera la utilización de esa rama. Al estar partida NDS el fallo de un servidor afecta sólo a parte de los recursos, aunque, en cualquier caso, existen mecanismos de réplica que evitan estas situaciones.

Una vez que se crean las particiones y las réplicas correspondientes, es necesario establecer un mecanismo que sincronice los datos recogidos en todas las réplicas de una partición, proceso complejo teniendo en cuenta que pueden ser modificados aspectos distintos de un objeto en dos réplicas de una misma partición. Esto se logra con un sistema de sincronización de los servidores de nombre mediante un sistema de marcas de tiempo que emplean todos los servidores a la vez que éstos tienen todos sus relojes coordinados a través de un programa.

d) Administración de archivos.

Los archivos pueden ser administrados indicando si son compartidos o no, en el primer caso, los usuarios autorizados pueden acceder y escribir en ellos, pero de uno en uno.



Ilustración 14: Replicación: una partición de NDS puede estar replicada en varios servidores.

Anotaciones

Otra opción que ofrece este sistema operativo es el acceso a archivos compartidos con bloqueo de registro, lo que significa que varios usuarios pueden acceder a un archivo aunque escribiendo un registro diferente cada vez.

Nota:

Los derechos de acceso a un determinado archivo son independientes de los derechos de acceso del objeto que representa ese archivo en NDS.

e) Seguridad del sistema.

Las redes Novell disponen de varios niveles de seguridad:

- Login: acceso a cualquier servidor introduciendo el nombre de este, el nombre de usuario y la clave de acceso. Si no se introducen correctamente estos datos el usuario es rechazado.
- Permisos de acceso: un usuario dispone de una serie de permisos en los distintos directorios, una vez que el usuario se ha identificado para acceder a un servidor podrá leer, escribir, borrar archivos, crear o modificar subdirectorios, etc.
- Permisos de directorio de manera que se controle el acceso a estos por parte de cualquier usuario. Cada usuario puede determinar las condiciones en las que comparte un determinado archivo. Estas condiciones se denominan atributos de archivo.

f) Administración de impresión.

Netware lleva implementado distintas opciones para administrar la impresión en red. El más importante es CAPTURE que se encarga de redirigir en el equipo local los trabajos de impresión que se envían a LPT1 hacia cualquier impresora de la red.

Además incluye el producto NDPS (Novell Distributed Print Services) que permite una gestión más eficaz de las impresoras a través del Netware administrador.

Las impresoras pueden conectarse directamente a la red, a un servidor de impresión, un servidor de archivos o un equipo cliente. NDPS permite controlar todas las impresoras de la red y redirigir los trabajos de impresión en función de la carga que esté soportando cada elemento del sistema.

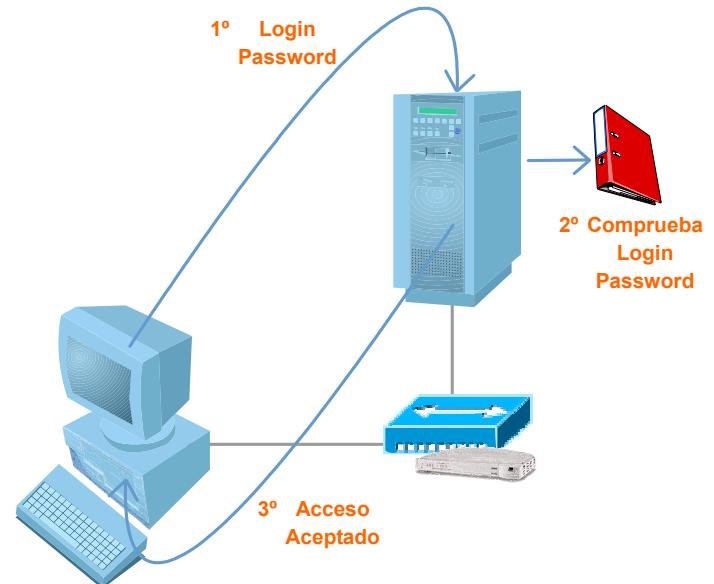


Ilustración 15: Niveles de seguridad: petición de acceso a un servidor y consulta de este a NDS para dar el permiso

Anotaciones

2.2. Protocolo IPX/SPX.

Cuando se crearon las redes Novell era habitual que se trabajara con sistemas propietarios, por lo que esta empresa desarrolló su propio protocolo de comunicaciones. Este protocolo fue denominado *Internetwork Packet Exchange / Sequential Packet Exchange* (Intercambio de Paquetes en Redes/Intercambio de Paquetes secuenciales).

Este protocolo se emplea únicamente en redes Novell. Fue en el pasado uno de los modelos de red más extendidos, actualmente también lo está, pero, debido al desarrollo de Internet está siendo sustituido por TCP/IP. Los principales protocolos de esta familia son IPX y SPX, de aquí su nombre. El sistema operativo Windows los incluye en sus opciones de red para facilitar la intercomunicación con las redes Novell.

Nota:

Hasta 1998 no se integraron de una forma nativa la pila de protocolos TCP/IP en el sistema operativo NetWare. Al mantener cerrados los detalles de funcionamiento de este protocolo Novell a perdido la batalla de la extensión de este protocolo como estándar de la industria.

La IPX/SPX, es *enrutable*, por ello hace posible la comunicación entre ordenadores que pueden pertenecer a distintos tipos de redes, interconectadas entre sí por encaminadores (routers), aunque en origen estaban orientados a redes LAN, empleando para identificar los equipos la dirección física de la tarjeta de red. Es una pila de protocolos que, debido a las limitaciones de origen, carece de la escalabilidad y universalidad de TCP/IP.

Para pensar:

Si IPX/SPX utiliza para identificar un host la dirección física. ¿deberán emplear algún otro mecanismo para identificar cualquier equipo destino de datos?

Las funciones de los protocolos IPX/SPX, se corresponden con los TCP/IP:

- **IPX** se corresponde con **IP**, y como él, trabaja en la capa de red. Se encarga del envío de los paquetes desde el origen al destino.

SPX se corresponde con **TCP**, y como él, trabaja en la capa de transporte. Se encarga del flujo de la transmisión y que los paquetes lleguen sin errores a su destino.

Nivel OSI	Protocolos de la pila IPX/SPX			
Presentación	NCP	SAP	RIP	
Aplicación			NetBIOS	
Sesión			Secuenciación de paquetes intercambiados SPX	
Transporte			Intercambio de paquetes internet IPX	
Red	Protocolos de acceso Ethernet, Token Ring, ARCnet			
Enlace	Cable coaxial, par trenzado			
Físico				

Ilustración 16: Relación entre el modelo OSI y la pila de protocolos IPX/SPX

Anotaciones

a) Serie de protocolos Netware.

Netware soporta los siguientes protocolos:

- **Internet Packet Exchange (IPX).** Protocolo de conexión de nivel 1 (equivalente al nivel 3 de OSI) que proporciona servicio sin conexión.
- **IPX Routing Information Protocol (RIP).** Protocolo de conexión de nivel 2 (nivel 4 de OSI) que proporciona al router la capacidad de mantener dinámicamente información de routing para IPX internetwork.
- **IPX Error Protocol.** Protocolo de conexión de nivel 2 (nivel 4 de OSI) que reporta errores en el procesamiento de paquetes. El error de notificación se envía desde el host o el router/bridge que detecta el error, al host Origen de los paquetes.
- **IPX Echo Protocol.** Protocolo de conexión de nivel 2 (nivel 4 de OSI) que se usa para verificar la operación de los dispositivos de la red. Comúnmente conocido como IPX ping.
- **IPX Service Advertisement Protocol (SAP).** Protocolo de conexión de nivel 2 (nivel 4 de OSI) que avisa a servicios de red, por ejemplo servidores de ficheros o servidores de impresoras.

b) Protocolo IPX.

El paquete IPX debe tener un máximo de 576 bytes, de ellos 512 bytes son para los datos, el resto es información necesaria. Cuando se trata de una red local, sin salida a exterior, pueden modificarse estos valores. IPX proporciona dos funciones: la primera es el *formateo de paquetes y entrega de datos* y la segunda reside en el *encaminamiento* hacia host de la misma red, o bien, de otra diferente (“routing”)

Un datagrama IPX contiene los siguientes datos:

- **Checksum:** Esta función no está activada en los datagramas IPX, aunque al proceder de la variación del protocolo IDP de Xerox, lo mantiene con el valor hexadecimal ffff.
- **Longitud:** indica la longitud total del paquete, incluida la cabecera. Ocupa 2 bytes.
- **Control de transporte:** cuenta el número de routers que atraviesa el paquete en su camino. El máximo número saltos es 15, pues al llegar a 16 el paquete es descartado. Este campo tiene un tamaño de 1 byte.

Tamaño	Campo
2 bytes	Check sum
2 bytes	Long. paquete
1 bytes	Control transporte
1 bytes	Tipo
4 bytes	Red destino
6 bytes	Nodo destino
2 bytes	Socket destino
4 bytes	Red origen
6 bytes	Nodo origen
2 bytes	Socket origen
Variable	Datos

Ilustración 17: Formato de datagrama IPX

Anotaciones

Para pensar:

¿Sabrías explicar la relación entre el tamaño del campo y el número máximo de saltos que admite este tipo de protocolos?

- **Tipo de paquete:** indica el servicio de nivel superior que ha originado el paquete de datos (desconocido, RIP, SAP, SPE o NCP), su tamaño es de 1 byte.
- **Red de destino:** contiene la dirección de la red a la que pertenece el host de destino. Dependiendo de esta dirección, un host o router sabe si hay que enviar el paquete a un host de la red local, o a un router que reenvíe el paquete a otra red. Tamaño 32 bits.
- **Host destino:** contiene la dirección física del host de destino. En una red Ethernet es el NIC de la tarjeta de red. Tamaño 48 bits.

Para pensar:

¿Cuántos bytes son 48 bits?

- **Socket destino:** indica el proceso al que se quiere acceder en el host destino. Tamaño 16 bits.
- **Red origen:** indica la dirección de la red origen. Tamaño 32 bits.
- **Host origen:** contiene la dirección física del host origen. Tamaño 48 bits
- **Socket origen:** indica el proceso que ha iniciado la comunicación. Tamaño 16 bits.
- **Datos:** se trata del campo del datagrama que incluye todos los datos, su tamaño es variable

Direccionamiento.

El direccionamiento de un paquete IPX está constituido por tres partes:

1. **Dirección de red:** son direcciones de 32 bits de LAN o WAN acoplada al nodo. Los nodos pueden estar conectados a varias redes, pero cada red debe tener una única dirección. Esta es la dirección que se informa a RIP.

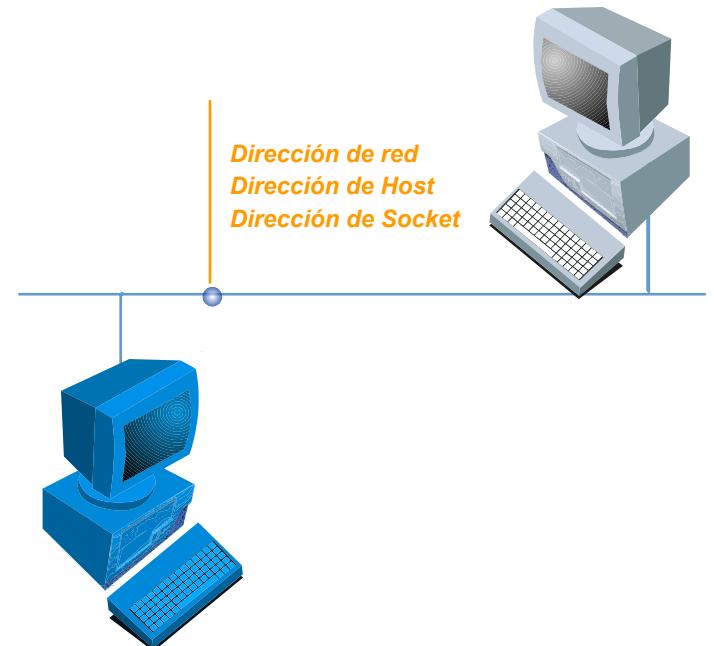


Ilustración 18: En las redes Novell se requieren tres direcciones distintas para el envío de un datagrama.

Anotaciones

2. **Dirección de host:** especifican la dirección física del nodo de la red y la correspondiente a la dirección de MAC. El router/bridge automáticamente usa la dirección de 48 bits de sus interfaces como direcciones de host. Esto es debido al esquema de direcciones en el que las interfaces de WAN de router necesitan una dirección de MAC cuando se configura un routing XNS o IPX.
3. **Dirección de socket:** son la localización de un proceso en la estación final o el host. El router/bridge no altera o manipula de ningún modo la dirección de socket.

c) Protocolo SPX.

Se trata de un protocolo de nivel de transporte del modelo OSI, que proporciona un servicio orientado a conexión y fiable de forma similar a TCP. Sin embargo se emplea mucho menos que TCP en las redes Novell ya que muchas de las funciones de este protocolo son asumidas en este tipo de redes por el protocolo principal de Netware.

Este protocolo se encarga de establecer y mantener la conexión entre dos host mediante el envío periódico de mensajes.

Una cabecera SPX incluye los siguientes campos:

- **Control de la conexión:** campo que contiene un código dedicado a regular la comunicación de datos en ambas direcciones. Tamaño 1 byte.
- **Tipo de datos:** Indica el protocolo de nivel superior que ha generado los datos y el tipo de estos. Tamaño 1 byte.
- **Identificador de conexión origen:** Identifica la conexión en el host de origen. Es necesario tener en cuenta que un host puede mantener varias conexiones. Tamaño 2 bytes.
- **Identificador de conexión de destino:** Identifica la conexión en el host de destino. Tamaño 2 bytes.
- **Número de secuencia:** crea una secuencia numérica con el fin de ordenar los paquetes de datos. Tamaño 2 bytes.
- **Número de confirmación:** indica el número de secuencia que debe tener el siguiente paquete de datos que reciba el sistema. Tamaño 2 bytes.

Tamaño	Campo
1 byte	Control de la conexión
1 byte	Tipo de datos
2 bytes	Id. De conexión de origen
2 bytes	Id. De conexión de destino
2 bytes	Número de secuencia
2 bytes	Número de confirmación
4 bytes	Número de asignación
Variable	Datos

Ilustración 19: Formato de paquete de datos SPX

Anotaciones

- **Número de asignación:** Indica el número de búferes libres del sistema. Tamaño 2 bytes.
- **Datos:** Campo que incluye los datos del proceso de nivel superior.

d) Protocolo principal de Netware (Netware Core Packet)

Es el protocolo que se encarga de gestionar la mayor parte del tráfico en una red Novell. Lo utilizan tanto los equipos clientes como servidores para enviar solicitudes y respuestas de archivos o enviar trabajos a la cola de impresión.

Trabaja desde el nivel de transporte hasta el nivel de presentación ya que se encarga tanto de aspectos de transporte (sustituyendo tal como ya se ha indicado al protocolo SPX) como de funciones superiores de sincronización o de bloqueo de archivos.

Existe el protocolo NCPB (Netware Core Packet Burst) con características similares al NCP pero que se utiliza para enviar gran cantidad de datos por la red, es el protocolo principal de ráfagas de paquetes de Netware y aporta grandes ventajas con respecto a otros protocolos del nivel de transporte, por ejemplo, envía y recibe sólo los fragmentos de datos perdidos sin necesidad de repetir toda la secuencia.

e) El Protocolo de Notificación de Servicios (SAP).

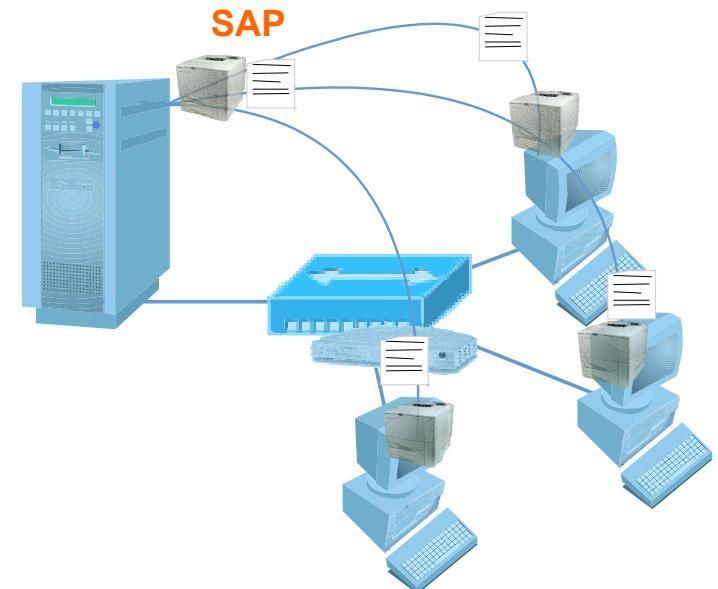
Para que la comunicación sea posible, es necesario conocer el nombre de un determinado servidor y el tipo de servicios que proporciona. Los nombres son más manejables que una serie de números, por eso los routers tienen un servidor de nombres, que relacionan las direcciones numéricas con su nombre, mediante un proceso denominado protocolo de notificación de servicios (SAP).

Los paquetes SAP los usan los servidores para informar a los routers y otros servidores de sus servicios, ya que ellos son los que se encargan de mantener las tablas de información acerca de estos servicios. SAP es un protocolo que utiliza encapsulación IPX. Cuando se inicia un servidor informa de sus servicios mediante paquetes SAP. Lo mismo ocurre cuando se desconecta, para que se elimine de las tablas de los routers.

f) RIP. Protocolo de Información de Encaminamiento de IPX.

Las funciones de RIP son:

- Encontrar la ruta más corta entre los diversos routers.
- Actualización de las tablas de encaminamiento de los routers.



Anotaciones

g) Configuración IPX sobre el router/bridge.

Existen tres métodos de configuración y mantenimiento de las tablas de routing:

- **Dinámico:** donde la información de routing de la red es trasladada entre routers utilizando el protocolo RIP.
- **Estático:** donde la información de routing es entrada manualmente, para proporcionar una ruta fija para una red, vía un gateway determinado. Cada ruta estática puede ser cambiada por una ruta aprendida dinámicamente por RIP.
- **Rutas por defecto:** que son entradas manualmente para proporcionar una ruta para la red de destino cuando esta no puede ser encontrada en la tabla de routing.

Para regular el flujo de tráfico, se usan unos filtros de control de acceso, que pueden restringir la comunicación entre dispositivos/redes. La restricción es entre la *red Origen y dirección de host*, y la *red destino y la dirección de host*. Adicionalmente las restricciones de comunicación pueden extenderse para aplicarlas a grupos de redes y/o hosts.

h) Encaminamiento IPX. Routers Novell.

La función de encaminamiento de los routers permite dirigir los paquetes hacia las diferentes redes. Hay dos tipos de routers en una red Novell que se han denominado a partir de las versiones 3.x como **routers internos y externos**. En los primeros se incluye la función de encaminamiento con servicio de ficheros e impresión. Los externos están constituidos por una estación de trabajo que incluye múltiples tarjetas de comunicaciones con la única función de dirigir paquetes.

Se pueden utilizar cualquier tipo de routers siempre que soporten protocolo IPX. Cuando se produce una alta especialización de comunicaciones se construyen propiamente eliminando en dichas funciones los computadores personales. Cada router necesita conocer todos los demás routers accesibles en su red. Mantienen una lista de las redes a las que tienen acceso, la cual se conoce como *tabla de encaminamiento*:

Cada red, está definida por su *número de red* constituidos por 32 bits, está separada de las otras mediante un router, siendo el conjunto de estas redes la denominada interred. Cada router tiene su tabla de encaminamiento y estas son transmitidas de unos routers a otros mediante paquetes RIP. Un router, está conectado con dos segmentos de red, llamados "*segmentos directamente conectados*". Inicialmente, un router configura una tabla con los números de las redes a las que está conectado directamente. A partir de este momento se envían mensajes "broadcast" a las redes conocidas del router, para conocer las tablas de los routers cercanos. Así se actualiza la tabla de los router.

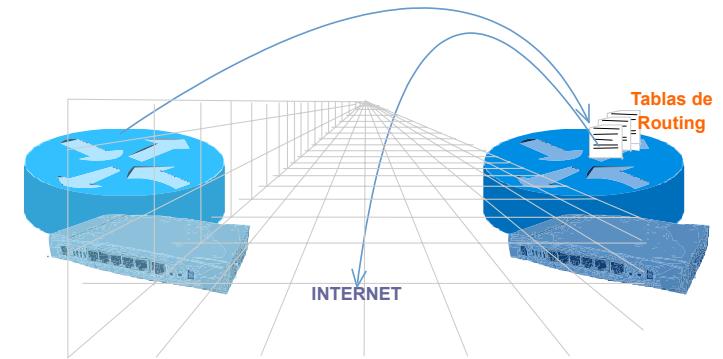


Ilustración 21: Función de RIP: RIP permite enviar las tablas de routing de un dispositivo a otro

Anotaciones

3. Redes de Microsoft Windows.

3.1. Características de las redes Windows..

Las redes gestionadas por sistemas operativos Windows son redes entre iguales que pueden funcionar con independencia de la existencia o no de un equipo servidor. En este sistema, todos los ordenadores pueden actuar como clientes o servidores dentro de la red montando distintas versiones de sistemas operativos.

Cuando incluimos un equipo servidor, con software de sistema operativo servidor, podemos crear sistemas de acceso más seguros a la red, administrarla de una forma centralizada y aportar una serie de servicios añadidos en función de la versión de sistema operativo instalada.

Las redes Windows son ahora las más utilizadas debido a la facilidad de su instalación y a la similitud de procesos e interfaces con las versiones de usuarios.

Pasamos a conocer sus características básicas.

a) Gestión de discos.

La gestión de discos de Windows es bastante conocida en sus aspectos básicos debido a que es el sistema operativo más utilizado. Un disco físico debe ser particionado, dimensionado y formateado.

Una partición es una unidad de almacenamiento separada, es decir, en ella se puede instalar un sistema operativo, de este modo, un mismo PC puede incluir un disco con, por ejemplo, tres sistemas operativos, debiendo seleccionar con cuál queremos trabajar. Además de las particiones primarias podemos crear particiones extendidas, que no se formatean, pero que se dividen en unidades lógicas. Este sistema de almacenamiento requiere que configuremos una partición primaria como partición activa, de esta forma indicamos dónde vamos a instalar los archivos de inicio del sistema operativo.

Todo lo que acabamos de comentar es posible cuando empleamos un sistema de almacenamiento básico, el existente hasta la aparición de Windows 2000.

Windows 2000 incorpora un nuevo sistema de almacenamiento, el almacenamiento dinámico que permite crear una única partición en lo que denominaríamos un disco dinámico, pero que puede ser dividido en volúmenes. La ventaja de los discos dinámicos es que podemos crear volúmenes que se extiendan a lo largo de distintos discos.

La selección de un determinado sistema de volúmenes estará vinculado con la tolerancia a fallos que presente.

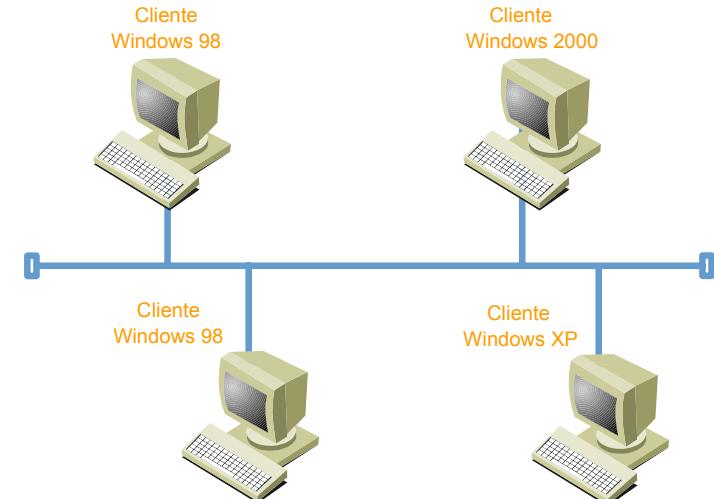


Ilustración 22: Las redes Windows pueden funcionar con independencia de un equipo con software servidor

Anotaciones

- **Volumen simple:** Se encuentra en un único disco y se puede extender hasta un máximo de 32 regiones. No es tolerante a fallos.
- **Volumen distribuido:** Volumen que se reparte a lo largo de varios discos dinámicos. No es tolerante a fallos. Se escribe en los discos de forma consecutiva, una vez que se llena la parte de volumen de un disco se pasa a escribir en otro.
- **Volumen con espejo:** Para lograr tolerancia a fallos un sistema es crear un volumen de este tipo, que se compone de dos volúmenes simples en el que uno es una copia idéntica del otro.
- **Volumen seccionado:** Un volumen se distribuye a lo largo de varios discos dinámicos pero la escritura se distribuye en todos ellos, no se van llenando discos de forma secuencial. No es tolerante a fallos. Mejora el volumen distribuido pues permite una escritura y lectura más rápidas.
- **Volumen RAID-5:** Con un mínimo de tres discos duros se crea un volumen seccionado pero se añade información a cada partición de disco en el volumen de manera que se evita la pérdida de datos.

El sistema de discos dinámicos no se puede configurar como partición activa del disco aunque sí pueden incluir archivos del sistema operativo de manera que se garantice su tolerancia a fallos.

b) Sistema de archivos.

Los sistemas operativos Windows pueden emplear como sistemas de archivos FAT16, FAT32 y NTFS. La utilización de uno u otro sistema va a permitir desarrollar o no una serie de posibilidades de utilización de ese mismo sistema operativo.

No todas las versiones de Windows soportan todos los sistemas de archivos enumerados, así, sólo las versiones de Windows NT, Windows 2000 y Windows XP pueden instalarse sobre discos formateados con NTFS, mientras que todas las versiones desde Windows 95 en adelante se pueden instalar en FAT 32, MS-DOS y Windows 3.x son totalmente compatibles con FAT16, únicamente.

Los sistemas de archivo permiten determinar, entre otras cosas dónde se ubica cada una de las partes de un archivo, ya que, debido a la forma en que se escribe en los discos, los distintos ficheros no aparecen completos en las unidades de escritura (clusters) ni consecutivos.

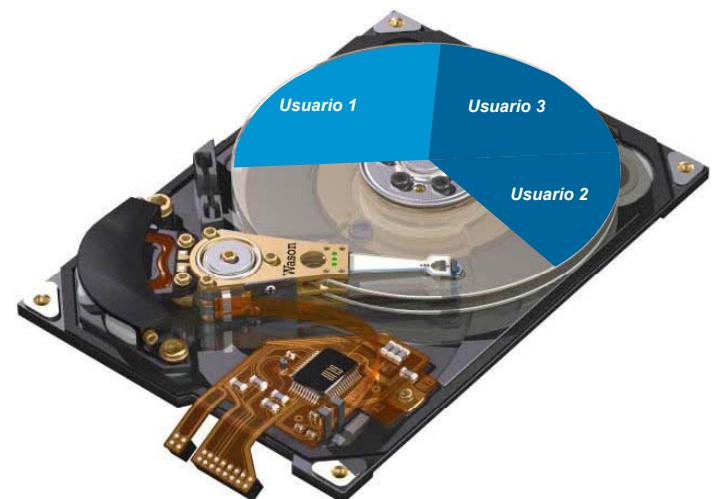


Ilustración 23: NTFS permite asignar distinto espacio de disco a cada usuario

Anotaciones

Nota:

Un cluster es la unidad mínima de almacenamiento que asigna el sistema operativo

FAT16.

Divide el disco en volúmenes y crea como unidades mínimas de escritura los cluster, que han de disponer de un tamaño fijo dependiente del tamaño de la partición. Los directorios que incluyen las unidades presentan, entre otros datos, la entrada en la FAT referida al cluster donde se inicia cada archivo. En esa misma entrada se indica otra entrada donde se señala cuál es el siguiente cluster del archivo, y así sucesivamente.

Para pensar:

Fat 16 admite numerar las entradas desde 0000000000000000 hasta 1111111111111111, es decir, admite 2^{16} clusters. Como cada cluster puede tener un tamaño máximo de 32768 bytes. ¿Cuál sería el tamaño máximo de una partición FAT16?

Como no se trata de un sistema de archivos de red, no permite almacenar información que utilizan los sistemas operativos compatibles con el trabajo en red, como características de una carpeta y control de acceso a usuarios.

Analogía:

Este documento debe ser guardado en un archivador, sin embargo, el archivador sólo admite un número determinado de páginas en cada departamento. Como ya está ocupado en parte, no podemos meter todo el documento en un mismo departamento, hay que irlo incluyendo página a página donde se puede. Evidentemente, es una locura, ya que tendría que recordar dónde he metido cada página y el orden en las que las debo leer.

Esta es la función del sistema de archivos, indicar dónde está y en qué lugar debo leer cada parte de mi documento.

FAT 32.

FAT 16 no admitía un tamaño de disco superior a dos Gbytes debido al tamaño de los cluster que creaba. FAT 32 permite tamaño de clusters más pequeños, proporcionando una gestión del disco mejorada, pero no admite ninguna opción de red. Se limita a proporcionar:

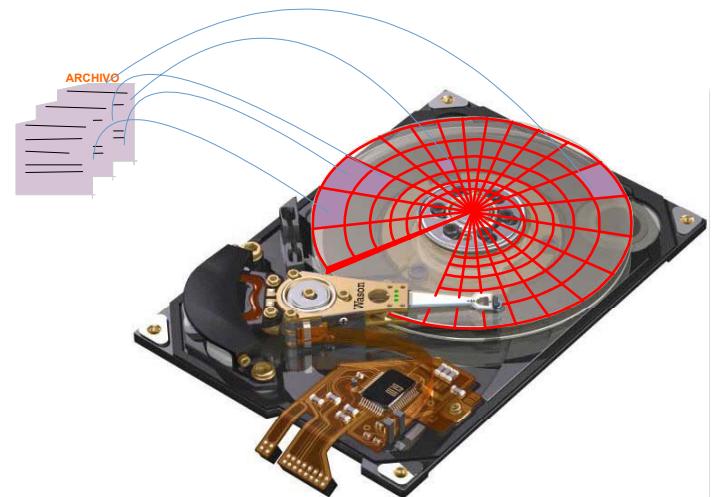


Ilustración 24: Un mismo archivo se encuentra dividido en distintos “Clusters” que deben ser localizados

Anotaciones

- Nombre de archivo.
- Atributos.
- Fecha/hora.
- Tamaño.

NTFS.

Es el sistema de ficheros que incorporó la primera versión de Windows NT para solucionar los problemas que presentaban FAT16 y FAT32. Incorpora características de almacenamiento avanzadas: seguridad, compresión y mejor gestión del disco.

La versión que incorpora Windows 2000, NTFS 5.0, mejora las capacidades iniciales de versiones anteriores incluyendo cuotas de disco por usuario (esta opción estaba disponible en Netware desde hacía años), cifrado de archivos y puntos de reanálisis.

Este sistema de ficheros es necesario cuando se desean incorporar a una red opciones de seguridad y gestión centralizada de directorios en sistemas Windows, de ahí, que se deba incorporar en discos de equipos servidores y clientes de red, pues el Active Directory (sistema de gestión de objetos de la red) se puede implementar, únicamente, en este sistema de ficheros.

3.2. Sistemas servidores de Windows.

Desde la primera versión de Windows NT 3.1 los sistemas operativos servidores han sufrido una gran evolución. La utilidad de las redes de ordenadores, sus ventajas han provocado un enorme crecimiento de las redes, en número y extensión. Redes mayores requerían mayores prestaciones y requisitos de administración y seguridad.

Windows ha mantenido una carrera en el diseño de sistemas operativos servidores aportando ideas que han inspirado a otras empresas del mismo modo que distintas versiones de Windows pueden haber adaptado ideas de otros sistemas de red.

Los SO de servidor de windows son muy similares en su arquitectura a los SO clientes, el núcleo es prácticamente idéntico, sin embargo, se caracterizan por incorporar servicios añadidos. Por ejemplo, en la última versión de Windows 2003 Server se incluyen, entre otros, los siguientes servicios:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.

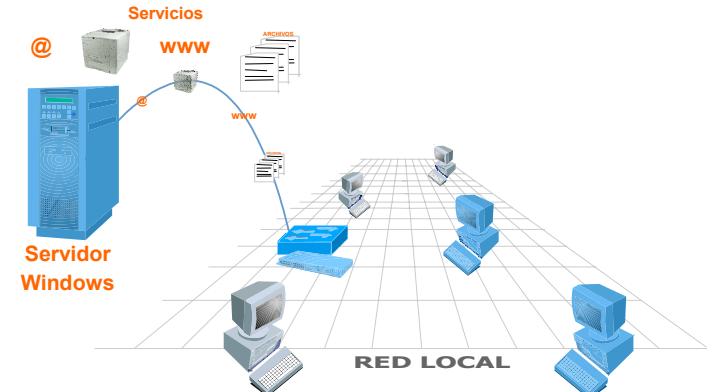


Ilustración 25: Servicio de Windows: puede proporcionar servicio de Correo, de archivos, de Web, de impresión, ...

Anotaciones

- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).

Estos servicios deben ser aprovechados por las estaciones de trabajo que se conectan a la red controlada por este servidor.

La evolución de este sistema nació en Windows NT, ha pasado por Windows 2000 y finaliza, por el momento, en Windows 2003 server. Sin embargo, cada uno de estos sistemas ha tenido distintas versiones que prestaban servicios distintos. Por ejemplo, de Windows 2000 server podemos hablar de las versiones: Small Business Server 2000, Advanced Server 2000, Datacenter Server 2000, además del Windows Server 2000.

Cada una de las versiones, tal como hemos indicado, incorporan distintos servicios, pero, además, presentan distintas capacidades en cuanto a soporte de procesadores y gestión de memoria.

En este tema nos vamos a centrar en las versiones más adecuadas para el trabajo en un centro.

a) Windows NT.

Windows NT posee un entorno muy similar a Windows 98, utilizan ambos la misma interfaz de red, los mismos protocolos, etc. En los dos sistemas se trabaja con la carpeta **Entorno de red**, de la misma forma.

La principal diferencia, es que Windows NT es un sistema operativo concebido como **servidor**, al contrario que Windows 98, que estaba concebido como **cliente**, aunque en ocasiones pueda hacer de servidor también. Windows NT, tiene un sistema de seguridad, con autenticación diferente. Exige una cuenta de usuario, con derecho de acceso a los recursos. Fue concebido para dar soporte a aplicaciones complejas que trabajan en modo multiusuario y con unos mecanismos de seguridad mínimos para la industria.

Windows NT tiene una versión diseñada para los puestos de trabajo (*Windows NT Workstation*) y una familia de versiones para trabajar en los servidores (*Windows NT Server*).

Características de Windows NT.

Las principales características son:

- **Sistema operativo a 32 bits:** Windows NT se creó para trabajar desde el principio con 32 bits, dejando en el olvido los sistemas anteriores de 16 bits.

Anotaciones

- **Sistema de archivos NTFS (New Technology File System):** Es un sistema de almacenamiento de archivos que incorpora seguridad en archivos y directorios. Controla mejor la fragmentación de archivos. Windows NT también incluye soporte para FAT (aunque no para FAT32) y HPFS (sistema de archivos de OS/2).
- **Multiusuario:** Un servidor con Windows NT, permite el acceso de varios usuarios a la vez desde distintos puestos de la red. Cada usuario puede ser propietario de objetos (carpetas, servicios, etc.) y, por ello, pueden administrar y controlar el acceso a estos objetos.
- **Multitarea:** Permite la ejecución simultánea de distintas aplicaciones. Aunque el procesador atienda únicamente una tarea en cada momento. Esto aumenta la velocidad enormemente.
- **Multiprocesador:** Puede soportar varios procesadores en el mismo ordenador, y cada uno trabajando a la vez con una tarea distinta.
- **Espacios de memoria separados:** Windows NT, se creó a partir de un núcleo experimental de UNIX, llamado Mach OS, que trabaja en modo *multihébra* y con derecho preferente. Debido a esto, además de una tecnología de *subsistemas protegidos*, puede trabajar con programas y aplicaciones en espacios de memoria separados. Esto impide que cuando falla un programa se produzca el fallo del resto de programas en ejecución. Se puede abortar dicho programa sin afectar al resto de los programas en funcionamiento.

Para pensar:

En numerosas ocasiones, con sistemas operativos Windows 95 o 98, nos encontramos con que una aplicación falla y debemos reiniciar el equipo. Sin embargo los espacios de memoria separados nos permiten acceder al administrador de tareas y finalizar únicamente la aplicación que no responde.

- **Portabilidad:** Windows NT puede funcionar en distintos tipos de hardware.
- **Trabajo en entornos mixtos:** Windows NT puede trabajar en distintos tipos de redes, cada cual con su protocolo. Por ejemplo: Novell Netware con IPX/SPX, Unix mediante TCP/IP, Macintosh con AppleTalk, Windows mediante NetBEUI, etc.

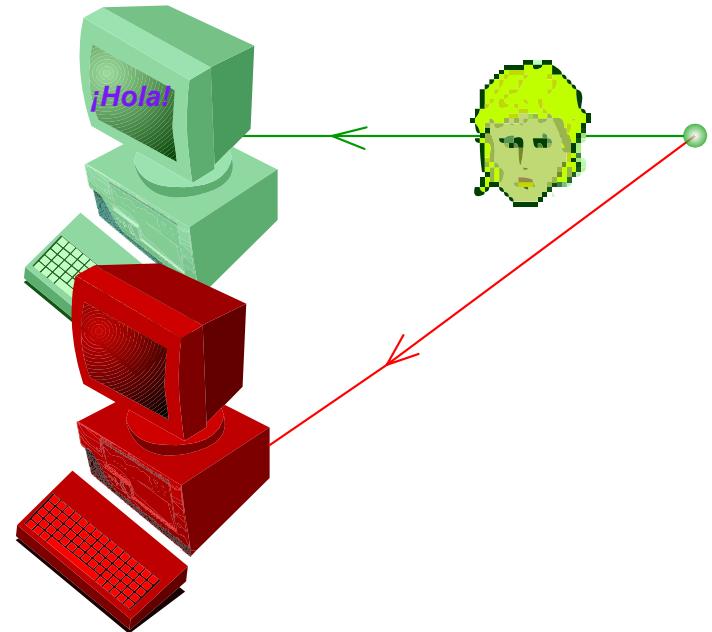


Ilustración 26: Control de acceso a los recursos en redes de "igual a igual": cada usuario controla el acceso a sus carpetas, administra sus objetos

Anotaciones

- **Validación en un dominio:** Los controladores de dominio son los ordenadores que se encargan de la autenticación de los usuarios de ese dominio. Para ello tiene una base de datos de usuarios o SAM (Security Account Manager). De esta manera, el acceso a los recursos de la red está controlado.
- **Tolerancia a fallos.** Windows NT posee mecanismos para trabajar aunque se produzca algún fallo. Un mecanismo orientado a esto es RAID (*Redundant Array of Inexpensive Disk*), que controla la pérdida de datos, incluso cuando falle el disco duro del ordenador.

Arquitectura de Windows NT.

Windows NT usa un modelo de objetos modular, con varios componentes, cada uno de los cuales tiene encargada una tarea específica dentro del sistema operativo. Una forma característica de trabajo de Windows NT, son los llamados *subsistemas de ambiente*, por los cuales se puede trabajar con diversos sistemas operativos emulándolos. Así, Windows NT, puede trabajar con DOS, OS2, POSIX, Win 16, etc.

Otro elemento característico son los llamados *Servicios Ejecutivos*. La función de estos es ejecutar una serie de funciones relativas a: procesos y hebras, seguridad, memoria, entrada/salidas, etc.

Windows NT, utiliza un sistema de *paginación de memoria virtual*, según demanda, con un direccionamiento lineal de 32 bits. Con este modelo se puede dirigir hasta 2GB de memoria RAM directamente, en vez de los segmentos de 64 MB, de los anteriores sistemas operativos. Con esto se pueden manejar aplicaciones y datos mucho más grandes.

Los datos se *paganan*, en páginas de 4K, moviéndose estas páginas entre la memoria física y un archivo en disco temporal, según lo vayan necesitando los programas.

Trabajo en red.

Generalidades.

En Windows NT las funciones de red vienen ya integradas. Los ordenadores pueden operar como clientes o servidores, en una red de tipo cliente-servidor o punto a punto.

En una red NT, tenemos diversos componentes que pueden ser agrupados en las siguientes categorías: sistemas de archivos, protocolos de red y controladores de tarjetas de red.

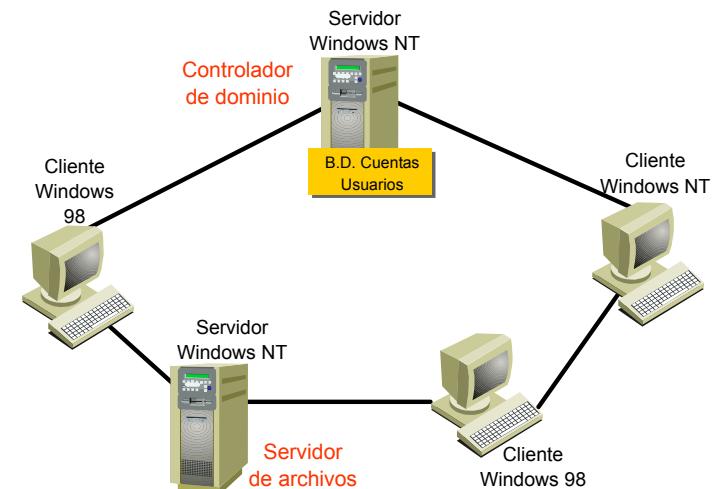


Ilustración 27: Un servidor NT controla la autenticación de usuarios para el acceso a un dominio

Anotaciones

NT trabaja en un modelo de capas de red que tiene su equivalencia con el modelo OSI de 7 capas:

- Los sistemas de archivos operan en el nivel de Aplicación y Presentación del modelo OSI.
- Hay diferentes protocolos para solucionar los problemas de las capas de sesión, transporte y red de OSI.
- Los controladores de las tarjetas de red se encargan de la comunicación entre ésta y el hardware y el software del ordenador. Estos controladores deben cumplir con la norma NDIS 3.0. Operan en el nivel MAC (Control de Acceso al Medio).
- La tarjeta de red opera en la capa física del modelo OSI.

Usuarios. Grupos de usuarios.

Un *usuario* es una persona que inicia una sesión de trabajo en Windows NT. El *usuario* viene definido por su *nombre de usuario* y su *contraseña*. Esto constituye la llamada *cuenta de usuario*.

Windows NT exige que todo usuario que inicie una sesión lo haga con un nombre de usuario y contraseña válidos, para ello tiene una base de datos de cuentas de usuarios, que utiliza para dar validez o no a un usuario.

Esta base de datos puede residir localmente en el propio ordenador del usuario. Lo más normal es que los usuarios se agrupen de una manera lógica, de acuerdo a algún criterio, en lo que se denomina *grupo de trabajo*, para ello se les asignará un *nombre de grupo*. Cada ordenador del grupo puede tener algún recurso compartido. Un grupo forma una red de “igual a igual” o “peer to peer”. En este caso, no hace falta que haya algún ordenador dedicado a contener la base de datos de cuentas de usuarios. Esta reside localmente en cada ordenador del grupo y se llama *base de datos de seguridad local*.

Cuando un usuario decide acceder a un dominio debe identificarse en un servidor del dominio, que contenga la base de datos de cuentas de usuarios. Este ordenador se denomina *controlador central de dominio* o *controlador de Dominio Primario* (conocido por su acrónimo en inglés, PCD). En este modelo, las cuentas se llaman *cuentas de dominio*, y se dice que los usuarios “inician una sesión en el dominio”.

Nota:

Un controlador de reserva de dominio BDC contiene una copia de seguridad del controlador principal, de manera que si éste falla, se activa el de reserva.



Ilustración 28: Control de acceso: En un grupo cada ordenador dispone de una base de datos de seguridad local en la que se identifican todos los usuarios, en un dominio la base se encuentra centralizada

Anotaciones

Un *dominio* es un agrupación lógica de ordenadores en red, que comparten una *base de datos de directorio (SAM)* situada en el controlador de dominio, que llevará *Windows NT Server*. SAM, contiene las cuentas de usuario del dominio e información de seguridad.

En un modelo de red con dominio, la administración del dominio es **centralizada**, ya que los recursos principales están centralizados, y la administración de ellos también. Aquí surge la figura del *administrador*, que es la persona que se encarga de la administración del dominio.

En Windows NT, a cada usuario se le adjudica un *permiso* o *privilegio*, sobre los recursos del sistema. Según el permiso que tenga un usuario podrá o no acceder a un recurso, y también nos dirá qué acciones podrá o no hacer (leer, escribir, imprimir, etc.). Cada usuario puede tener un *permiso* o *privilegio* individual, pero es más práctico crear grupos de usuarios que tengan los mismos privilegios.

Hay dos clases de grupos:

- *Grupo global*: es un grupo de usuarios del mismo dominio.
- *Grupo local*: puede contener grupos globales o usuarios del mismo o distintos dominios.

Recursos. Gestión de recursos.

Los principales recursos que tenemos en una red Windows son los datos, que están almacenados en *archivos* y estos, a su vez, en *carpetas*, y las *impresoras*. Los recursos pueden *compartirse*, para que los demás usuarios puedan disponer de ellos. El administrador puede definir las reglas y condiciones para acceder a los recursos. A esto lo denominamos *gestión de recursos*.

Cada recurso tiene una propiedad, llamada *compartir*, con ella podemos elegir qué recursos se quieren compartir, por quién, y de qué forma.

En cuanto a carpetas, podemos clasificarlas en:

- Carpeta pública: a ella pueden acceder todos los usuarios.
- Carpeta de grupo: a ella pueden acceder un grupo concreto de usuarios.
- Carpeta privada: a ella pueden acceder únicamente su propietario.

La gestión de una red consiste en definir los grupos de usuarios, los distintos tipos de carpetas y los distintos permisos que tendrán cada usuario y grupo para acceder a las carpetas.

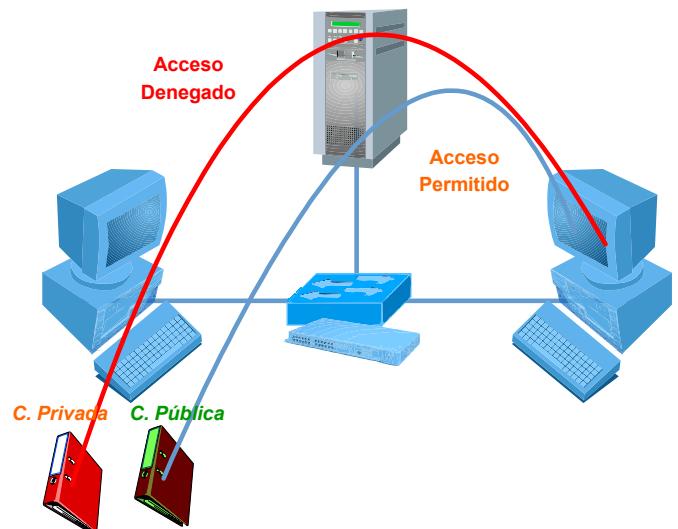


Ilustración 29: Carpeta pública y privada: una carpeta pública es aquella que es accesible al resto de los usuarios

Anotaciones

Seguridad de los recursos en Windows NT.

Windows NT protege sus recursos permitiendo el acceso a ellos solamente al usuario autorizado. A este modelo se le denomina *seguridad por usuario*.

Los recursos, en Windows NT, se consideran *objetos*. Por ejemplo: archivos, carpetas, procesos, impresoras, etc. Un objeto, en Windows NT, es el objeto en sí mismo y las acciones (leer, escribir, etc.) para manipular a dicho objeto. Cada objeto tiene asociado un ACL (Access Control Lists), que contiene las cuentas de usuarios y grupos que pueden acceder a dicho objeto.

Cuando un usuario intenta acceder a un objeto, Windows NT, compara el SID del usuario y del grupo al que pertenece con la información del ACL del objeto, y permite o no dicho acceso.

Analogía:

Un vigilante jurado en una empresa dispone de una lista de las personas que trabajan en ella, de las visitas que se esperan y de si se esperan envíos de algún tipo. Cada vez que llega alguien, le pide que se identifique y coteja la lista que dispone, si esa persona es de la empresa o se la espera para realizar alguna operación se le deja pasar.

Compartir impresoras.

En una red NT, se puede imprimir desde un servidor con Windows NT, como si lo hicieramos en una impresora local. Para ello, la impresora se debe haber definido como una impresora de red compartida. De esta forma aparece en el entorno de red como un elemento más.

Los usuarios tendrán que agregar esta impresora en su ordenador, y ya pueden imprimir en ella como si la tuviera conectada a sí mismo.

b) Windows 2000 Server.

Introducción a Windows 2000.

Windows 2000, sería en realidad la versión 5 de Windows NT, pero Microsoft decidió en esta versión cambiar de nombre a Windows 2000. Por tanto es una extensión de Windows NT, y tiene la misma filosofía.

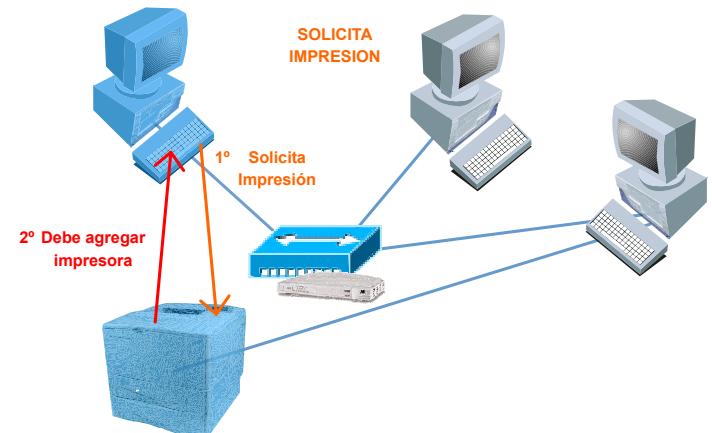


Ilustración 30: Para que un usuario pueda emplear una impresora la debe agregar a su equipo

Anotaciones

Anteriormente existían dos líneas de Windows; Windows 98 para redes punto a punto, trabajo en grupo o individual en un ordenador aislado; y Windows NT, para trabajo en red, con servidores y, normalmente, dentro de un dominio. En Windows 2000 convergen estas dos líneas.

Windows 2000 está concebido, al igual que Windows NT, para dar soporte a aplicaciones complejas que trabajan en modo multiusuario y con unos mecanismos de seguridad mínimos para la industria. Dispone de una versión diseñada para empresas y usuarios finales (*Windows 2000 Profesional*) y varias versiones con herramientas de administración y gestión de red (*Windows 2000 Server* es la versión más basica de los servidores Windows 2000).

Características de Windows 2000.

Además de las ya conocidas incorporadas por Windows NT:

- Sistema operativo a 32 bits.
- Sistema de archivos NTFS (New Technology File System).
- Multiusuario, multitarea, multiprocesador.
- Espacios de memoria separados.
- Modular.
- Portabilidad.
- Trabajo en entornos mixtos.
- Validación en un dominio.

Windows 2000 incorpora las siguientes características:

- **Seguridad:** Identificación de usuarios. Seguridad local y de red. Revisión de carpetas, impresoras, etc. El protocolo Kerberos, utilizado en Windows 2000, es un protocolo de autenticación de red, para transmitir datos a través de redes inseguras. Las *relaciones de confianza transitivas* de Kerberos, permiten a Win2000 crear árboles y bosques de dominios. Kerberos utiliza la *autenticación mutua*, el servidor y el cliente verifican la autenticidad de su compañero. Win2000 utiliza el sistema de clave pública (PKI). PKI es un sistema de certificados digitales y Certificate Authorities (CAs), que hace que en una transacción, las dos partes verifiquen la autenticidad de la otra y encripten la transacción. PKI se usa en Internet para el comercio electrónico seguro.

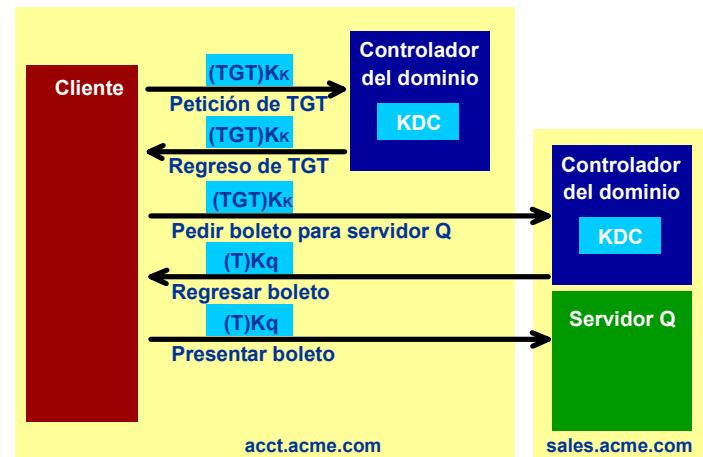


Ilustración 31: Kerberos: Funcionamiento del protocolo de autenticación de red

Anotaciones

- **Tolerancia a fallos.** Windows 2000 posee mecanismos para trabajar aunque se produzca algún fallo. Un mecanismo orientado a esto es RAID (Redundant Array of Inexpensive Disk), que controla la pérdida de datos, incluso cuando falle el disco duro del ordenador.
- **Integración con Internet:** Server incluye Internet Information Server (IIS), una plataforma segura de servidor Web.
- **Directorio activo:** sistema de servicios de directorio aplicable a redes ilimitadas en su tamaño. Mejora el sistema de Windows NT (SAM) y se asemeja al empleado en las redes Novell (NDS)

Arquitectura de Windows 2000.

Windows 2000, al igual que Windows NT, tiene dos capas, que separan en dos niveles las funciones. Cada capa tiene un modo de funcionamiento distinto: *modo Kernel*, con este modo se hacen las tareas más internas; y *modo usuario*, con el que se ejecutan las aplicaciones.

Modo Kernel o Núcleo:

El Kernel o Núcleo es, en Windows 2000, algo parecido al corazón. Hace de intermediario entre el sistema operativo y el procesador del ordenador. Tiene acceso al sistema de datos y al hardware y ejecuta en un área de memoria protegida. Sus principales componentes del núcleo son:

- 1) Executive Services: cada servicio se encarga de una función. Las principales son:
 - a) Administrar las Entradas/Salidas (I/O) hacia cualquier dispositivo.
 - b) Administrador de objetos: gestiona todos los posibles objetos utilizados por Windows 2000.
 - c) Administrador de procesos.
 - d) Administrador de memoria virtual.
- 2) HAL (Hardware Abstraction Layer) (Capa de Abstracción de Hardware): controla la interacción del Núcleo con el Hardware. Su misión, es abstraer o hacer que el sistema ignore, el tipo de hardware de la máquina. Windows 2000, no permite al software el acceso directo al hardware, siempre tiene que pasar por el HAL. Gestiona las interfaces de Entrada/Salida, controladores de interrupción y la comunicación multiprocesador.
- 3) Controladores del modo núcleo: son un conjunto de componentes modulares, cada uno con una función.

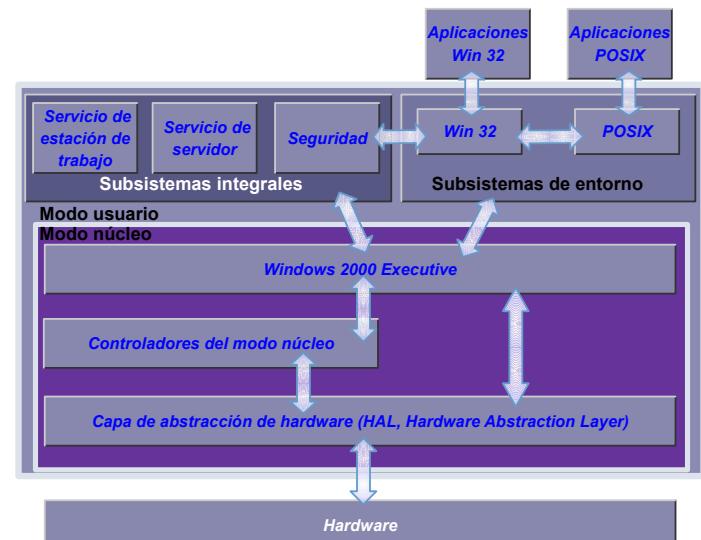


Ilustración 32: Arquitectura de Windows 2000

Anotaciones

Modo usuario:

En este modo, Windows 2000, usa un serie de subsistemas de entorno o ambiente, encargado cada uno de un tipo de aplicación, según el sistema operativo (Win32, OS/2, POSIX), emulándolos. Las aplicaciones y usuarios finales, no tienen porqué conocer nada de lo que pasa en el núcleo.

Cada programa se ejecuta en un espacio de memoria diferente, así no puede haber interferencias entre ellos.

Hay otra serie de subsistemas, llamados integrales, que gestionan la seguridad y el trabajo en red.

Servicios de directorio. Directorio Activo.

El Directorio Activo es una base de datos que almacena información sobre todos los recursos de la red y permite administrarlos. Nos da información sobre los recursos de la red, tales como usuarios, grupos, ordenadores, impresoras, etc. Estos recursos, son los llamados Objetos del Directorio Activo. Estos objetos son almacenados en unas Unidades Organizativas (OUs, Organizational Units) de forma jerárquica. Las Unidades Organizativas, se usan para organizar objetos dentro de un dominio, de manera parecida a una estructura empresarial.

Todos estos objetos forman una gran base de datos, que guarda información sobre usuarios, recursos y seguridad de la red. Permite a los administradores gestionar y controlar la red.

Un *Servicio de directorio*, proporciona los medios para la gestión de los diversos objetos del *Directorio*. Con él se pueden hacer:

- Administrar la seguridad de acceso a los diversos objetos de la red.
- Replicar o hacer copias de seguridad de un directorio en varios ordenadores.
- Repartir los diversos objetos de la red en distintos ordenadores.

Active Directory proporciona mejoras con respecto a SAM de Windows NT a la hora de administrar los objetos de una red. Mientras que SAM presentaba una estructura plana, en el que se gestionaban dominios, AD ofrece una estructura jerárquica en árbol, donde están representados todos los objetos de la red, que permite adaptarse mucho mejor a una red grande o en constante evolución. Aunque también trabaja con dominios, su principal ventaja es que éstos están integrados en la estructura y se pueden modificar dominios enteros de una forma sencilla.

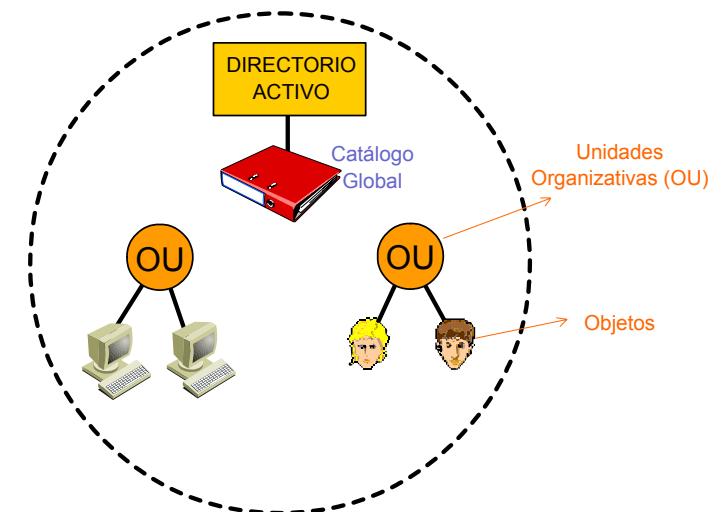


Ilustración 33: Active Directory es una base de datos que almacena de forma jerárquica los recursos de la red y permite su administración.

Anotaciones

Los dominios son las unidades organizativas básicas. Los dominios se pueden agrupar en árboles y los árboles pueden constituir un bosque. AD permite acceder, por ejemplo, a un árbol completo, con varios dominios y administrarlo como si fuera un único objeto. AD permite gestionar los usuarios de varios dominios simultáneamente, mientras que SAM sólo permitía gestionar los usuarios de un único dominio.

Como podemos observar, la estructura de Active Directory de Windows 2000 Server es muy similar a NDS de Novell. La estructura jerárquica en árbol dispone de objetos contenedores (Unidades Organizativas), que pueden incluir otros objetos denominados hojas.

La estructura de árbol que presenta active Directory no debe confundirse con la agrupación lógica que podamos hacer de usuarios o grupos, pues estos son objetos de Active Directory, no unidades jerárquicas.

Para pensar:

Windows NT permite con facilidad gestionar un dominio, pero si se dispone de más de dos conviene emplear Windows 2000 con Active Directory. La utilización de dos dominios, integrados en un mismo árbol, posibilita separar el centro en dos zonas independientes; los usuarios de un grupo pueden tener unos derechos en ambos dominios y otros sólo en uno de ellos. Por ejemplo, dominio de administración y dominio aula. En un centro bastaría con un árbol con uno o dos dominios.

Para evitar la pérdida de datos de Active Directory se emplea un sistema de reproducción de maestro múltiple, que permite que todos los datos sean actualizados automáticamente. Además de emplear un sistema de marcas de tiempo, parecido al de NDS, AD utiliza números de secuencia de actualización (USN). Cada vez que se hace un cambio en cualquier directorio se crea un USN, a la hora de actualizarse un controlador de dominio pide al resto de los controladores todas las modificaciones con USN superior al mayor de los que el dispone.

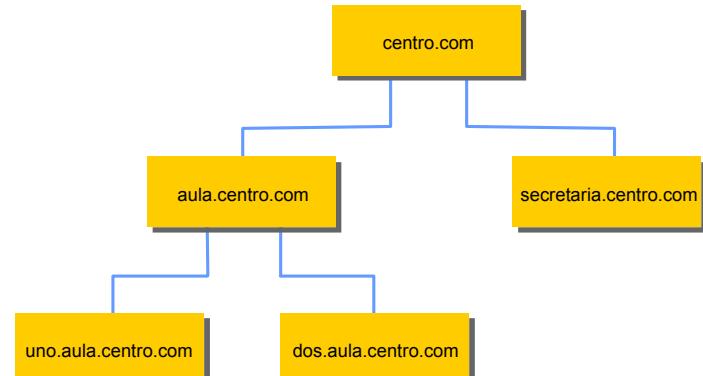


Ilustración 34: Diagrama de espacios de nombres de dominio

Anotaciones

Trabajo en red.

En Windows 2000 las funciones de red vienen ya integradas. Los ordenadores pueden operar como clientes o servidores, en una red de tipo cliente-servidor o punto a punto. Windows 2000 Server es un servidor de archivos, de aplicaciones, de impresión y servidor web.

Windows 2000 Server, tiene un elemento fundamental para el trabajo en red, el *Directorio Activo (AD)*.

Grupos de trabajo.

Cada ordenador del grupo, tiene una *base de datos de seguridad local*, con los usuarios y recursos del grupo. No hay una base de datos centralizada. Un *grupo de trabajo*, no necesita una administración centralizada, y no necesita tener instalado Windows 2000 Server en ningún ordenador, basta con Windows 2000 Profesional o 98. Es práctico para menos de 10 ordenadores.

Dominios.

Un *dominio*, es una agrupación lógica de ordenadores, que tienen una base de datos *centralizada*, o directorio. Esta base de datos contiene toda la información sobre los usuarios y recursos del dominio. En el *dominio*, hay siempre algún ordenador dedicado a contener el directorio, se le llama *controlador de dominio*.

El dominio, necesita una administración centralizada, y necesita tener instalado Windows 2000 Server en el controlador de dominio. Los ordenadores del dominio pueden estar próximos, o repartidos geográficamente por cualquier parte del mundo.

La característica esencial de un dominio es la *organización centralizada*, con todas las ventajas de control, seguridad y gestión que esto conlleva. El acceso a cualquier *objeto del dominio*, está controlado por el administrador, que define los derechos de acceso y la política de seguridad del dominio.

Los dominios se pueden agrupar jerárquicamente (padres, hijos) para formar un *árbol*. De esta forma los dominios del árbol pueden compartir información común. Hay un directorio único para todo el árbol, y cada dominio posee una parte de dicho directorio.

Los árboles se pueden agrupar en un *bosque*. Todos los árboles del bosque tienen un esquema y unas reglas comunes. Hay un *catálogo global*, con todos los objetos, para todos los dominios del bosque.

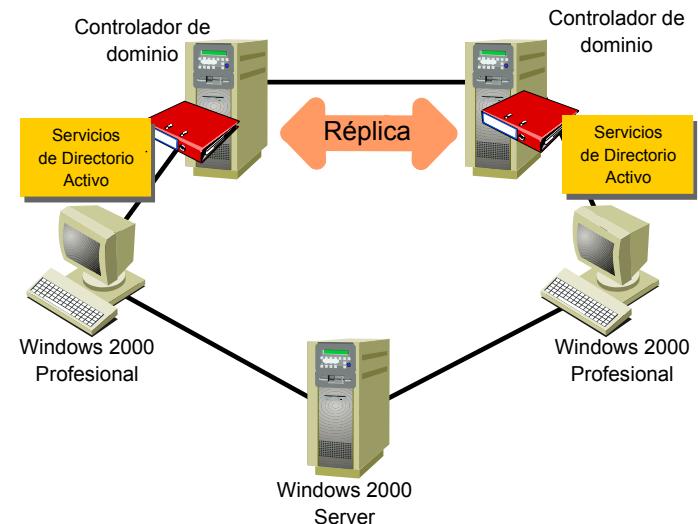


Ilustración 35: Dominio: Es una agrupación lógica de ordenadores que tienen una base de datos centralizada

Anotaciones

Sistema de Nombres de Dominio (DNS).

Windows 2000, usa el protocolo DNS para resolver (convertir) los nombres de los ordenadores, a direcciones de IP (Protocolo Internet). Windows 2000 también usa DNS para su servicio de nombres de dominio. De esta forma el protocolo DNS, permite utilizar el mismo sistema de nombres en Internet y en la red local, para nombrar los dominios. Windows 2000 emplea, igualmente, DNS Dinámico (Dynamic DNS, DDNS). Este protocolo, permite a los ordenadores clientes, que tienen direcciones IP asignadas dinámicamente (DHCP), poder registrarse directamente en un servidor DNS y actualizar la base de datos DNS. Este sistema, reduce la necesidad cambiar manualmente y replicar la base de datos DNS, cada vez que haya algún cambio en la configuración de un cliente.

DNS, utiliza una estructura jerárquica de nombres. Cada dominio tiene un nombre. Un dominio, en DNS, es un nodo que representa una partición de la base de datos de DNS. El nombre último, el de un ordenador concreto de una red (host), es el término situado más a la izquierda.

Nota:

Los dominios de administración de una red Windows no tienen por qué coincidir con el dominio público del centro, aunque deben ser gestionados con un servidor DNS

Control de acceso a objetos.

El modelo de seguridad de Windows 2000, se basa en el *control de acceso a los objetos*. Este control está basado en los **permisos**. Cada objeto del Directorio Activo, tiene definido qué tipo de acceso está permitido, y quién tiene permiso para acceder.

A efectos prácticos, se pueden agrupar los objetos en Unidades Organizativas (OU), para asignar los mismos permisos a todos los miembros de la OU. Los permisos para acceder a un objeto, los da el propietario del objeto o el administrador.

Cada objeto tiene una lista (ACL) de permisos de acceso, con los usuarios, grupos, etc. y tipos de permiso. También un *Descriptor de seguridad*, que podemos concebir como una “cerradura”. Cualquier usuario que quiera acceder a dicho objeto debe tener una “llave” para poder acceder. Cada usuario, al iniciar una sesión en un ordenador, obtiene una “llave”, la *Señal de acceso de seguridad (SAT)*. Con esta “llave”, podrá abrir unas “cerraduras” sí, y otras no, o sea, podrá, o no, acceder a los objetos.

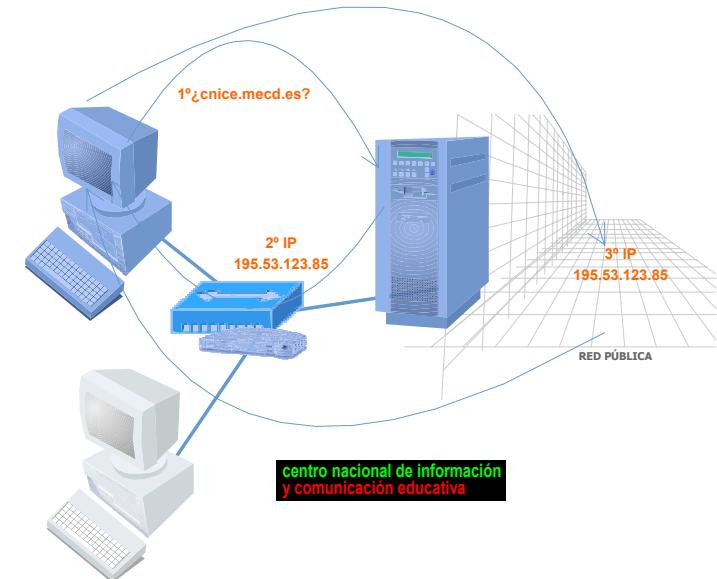


Ilustración 36: Sistema de nombres de dominio DNS: este protocolo, permite a los ordenadores clientes, que tienen direcciones IP asignadas dinámicamente , poder registrarse en un servidor DNS y actualizar la base de datos DNS

Anotaciones

Los permisos varían según el tipo de objeto. Por ejemplo, una carpeta puede tener permiso de lectura o escritura o para borrar; crear o modificar ficheros; mover un fichero de una carpeta a otra; etc.

Un usuario concreto, puede pertenecer a uno o varios grupos y, por tanto, tener los permisos correspondientes a cada uno de los grupos. Los permisos se pueden conceder o negar. Siempre tiene prioridad un permiso denegado. Cada objeto debe tener al menos un usuario, lo normal es el propietario o el administrador, que tenga un permiso *total*. Los permisos se pueden heredar, desde un objeto padre a un hijo. También se puede delegar un permiso, desde el administrador a un usuario o grupo.

Usuarios.

Un *usuario*, como este nombre indica, es una persona que inicia una sesión de trabajo en Windows 2000. Para poder trabajar (iniciar una sesión), en Windows 2000, se debe tener una **cuenta de usuario**. Esta es un registro, con el *nombre de usuario*, *contraseña*, grupos a los que pertenece y los permisos de acceso a los recursos del sistema. Windows 2000, no te deja acceder a la red si no te identificas.

Las cuentas de usuarios, se almacenan en una base de datos llamada *Administrador de cuentas de seguridad (SAM)*. Una cuenta de usuario, da la posibilidad de iniciar una sesión en un dominio, para acceder a los recursos de una red; o en un ordenador concreto, para acceder a los recursos de ese ordenador.

Una cuenta de usuario de dominio, está dentro de una Unidad Organizativa (OU), y estará almacenada en la base de datos del Directorio Activo, en un controlador de dominio. Si hay varios controladores de dominio, la información se duplica en cada uno. Una cuenta de usuario local, se almacena en la base de datos de seguridad (SAM) del ordenador, y no en el controlador de dominio.

Hay algunas cuentas de usuarios predefinidas, como el Administrador e Invitado. La cuenta de usuario Administrador, tiene privilegios para crear y modificar cuentas de usuarios y grupos, definir directivas de seguridad, asignar permisos, etc. La cuenta de usuario Invitado, se usa para usuarios ocasionales.

Para una cuenta de usuario determinada, se puede crear un Perfil de usuario, que contiene una serie de carpetas y configuraciones con datos personales.

Grupos de Usuarios.

Lo más normal es que los usuarios se agrupen de una manera lógica, de acuerdo a algún criterio, en lo que se denomina *grupo de trabajo*, para ello se les asignará un *nombre de grupo*. Un *grupo*, es un conjunto de cuentas de usuarios.

Anotaciones

Los grupos se crean para simplificar la administración de una red. Así, los permisos y derechos, se pueden asignar a grupos, en lugar de hacerlo individualmente, a cada usuario. Un usuario puede pertenecer a uno o varios grupos. Además de usuarios, un grupo puede contener contactos, ordenadores y otros grupos.

Los permisos son reglas asociadas a objetos, como carpetas, archivos o impresoras. Definen qué usuarios pueden acceder a dichos objetos y qué pueden hacer. Las acciones que se pueden hacer en una carpeta, pueden ser leer, modificar o crear archivos en su interior. En una impresora, pueden ser eliminar tareas, configurar, etc.

Los derechos son reglas que definen las acciones, que pueden hacer los usuarios, tales como, hacer una copia de seguridad de un ordenador, apagar el sistema, etc.

A cada usuario se le adjudica un *permiso* o *privilegio*, sobre los recursos del sistema. Según el permiso que tenga un usuario podrá o no acceder a un recurso, y también nos dirá qué acciones podrá o no hacer (leer, escribir, imprimir, etc.). Cada usuario puede tener un *permiso* o *privilegio* individual, pero es más práctico crear grupos de usuarios que tengan los mismos privilegios.

Tipos de Grupos.

Hay dos clases de grupos:

- *Grupo de seguridad*: son los utilizados para asignar permisos.
- *Grupo de distribución*: para funciones de correo. En este tipo de grupos no se pueden asignar permisos.

Ámbito de los Grupos.

Hay tres clases de grupos, según su ámbito de actuación:

- *Grupos locales de dominio*: son los utilizados para asignar permisos, para acceder a los recursos de ese dominio exclusivamente. Pueden contener miembros de otro dominio.
- *Grupo globales*: son los utilizados para agrupar usuarios del dominio desde el cual se crea el grupo, con las mismas necesidades de recursos de red. Pueden acceder a recursos de su dominio o de otros.
- *Grupos universales*: son los utilizados para asignar permisos, para acceder a los recursos de varios dominios. Pueden contener miembros de cualquier dominio

Anotaciones

Capítulo 5

Normas para la creación de los Grupos.

Se recomienda seguir los siguientes pasos:

1. Creación de los grupos globales, incluyendo a los usuarios de cada grupo.
Ejemplos: Contabilidad, Ventas.
2. Creación de los grupos locales de dominio, agrupando los recursos, y asignándolos a cada grupo local. Ejemplo: Impresoras color, Escáneres.
3. Agregar los grupos globales, que tengan que acceder a los recursos, al grupo local adecuado. Ejemplo: agregar Ventas a Escáneres y Contabilidad a Impresoras color.
4. Asignar los permisos pertinentes al grupo local de dominio.

Políticas o directivas de grupo.

Las políticas de grupo, son un conjunto de opciones de configuración de los ordenadores y de los usuarios. Estas opciones, se guardan en los objetos de políticas de grupos (Group Policy Objects, GPOs), y están asociados a objetos del Active Directory, tales como dominios o unidades organizativas. De esta forma se puede controlar el entorno de trabajo de un grupo de usuarios, una Unidad Organizativa o un dominio, de una forma centralizada.

En las directivas de grupo, se pueden incluir parámetros de software, de seguridad, programas disponibles a los usuarios, escritorio, acceso restringido a carpetas del sistema Windows 2000 , derechos de las cuentas de usuario, etc.

Se puede evitar que los usuarios instalen software o accedan a programas o datos no autorizados, que borren datos o programas importantes, etc.

Los administradores, son los que configuran estas directivas de grupo.

c) **Windows 2003 Server.**

Se trata del nuevo sistema operativo de Microsoft, heredero de Windows 2000 Server al que añade opciones que permiten una gestión más flexible de la red a la vez que se aumenta su seguridad.

Mejora la administración del Directorio activo y de las unidades de almacenamiento, tanto discos dinámicos como unidades extraíbles. Incorpora un servidor web y permite el alojamiento y creación de sitios XML web dinámicos. Se trata de la evolución natural de Windows 2000 Server ofreciendo opciones mejoradas e implementando tecnologías que han aparecido en los últimos años.

Anotaciones



3.3. Sistemas clientes de Windows.

El Sistema Operativo WINDOWS, incluye la opción de trabajo en red desde las versiones 3.1, con la extensión Windows para Trabajo en Grupo (Windows For Workgroups WFW), que proporciona las funciones necesarias para trabajar en una red punto a punto.

Las redes de Windows, son redes *punto a punto (peer to peer)*, es decir de igual a igual, y por lo tanto, cada ordenador puede trabajar como cliente, accediendo a algún recurso de la red, o como servidor, ofreciendo algún recurso, indistintamente, según las necesidades. Además tiene una serie de aplicaciones para hacer la red operativa y eficaz.

a) Windows 3.1

Se trata del primer sistema operativo Windows con posibilidades reales de trabajo en red. En las versiones anteriores era necesario conectarse mediante MS-DOS. Sin embargo todavía no es un sistema operativo completo, puesto que necesita de MS-DOS para funcionar.

Con Windows 3.1x nace el concepto de redes de igual a igual, donde cada ordenador puede trabajar como cliente, accediendo a algún recurso de la red, o como servidor, ofreciendo algún recurso, indistintamente, según las necesidades. Además, se integran una serie de aplicaciones para enviar correos electrónicos, trabajar en grupo, gestionar calendarios conjuntos y más, lo que convierte la red en un instrumento eficaz e útil.

Algunas características son:

- Trabaja con los protocolos IPX/SPX, NetBEUI, y TCP/IP.
- El sistema de almacenamiento en el disco duro es FAT, conocido también como FAT16. Realmente, es una tabla que el sistema operativo usa para localizar los archivos en las distintas secciones en las que está dividido el disco duro. Estas secciones se denominan “cluster” y sólo pueden almacenar un archivo. Si el archivo no ocupa todo el cluster, el espacio sobrante digamos que “se pierde” o se desperdicia. Cada cluster tiene una capacidad de 32K, entonces si el archivo sólo ocupara 5K, se perderían 27K.
- Necesita “correr” sobre MS-DOS. No es por lo tanto un sistema operativo completo por sí mismo.
- Utiliza una interfaz gráfica con menús desplegables que trabaja con ventanas.
- Soporte para uso en red.
- Soporte para el funcionamiento de archivos multimedia.

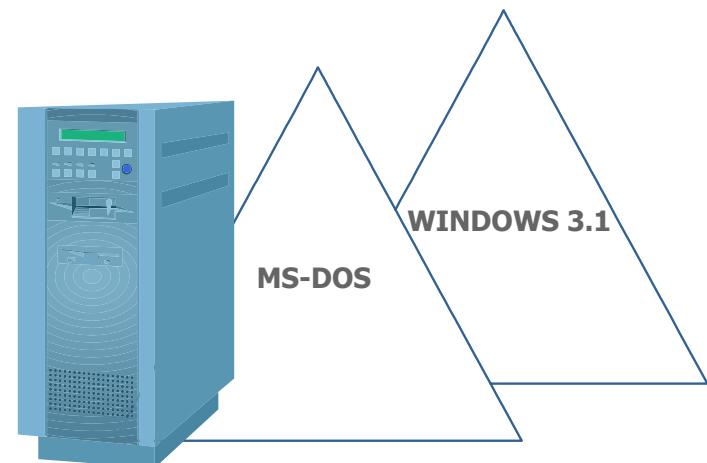


Ilustración 37: Windows 3.1: necesita de MS-DOS para poder operar con el hardware

Anotaciones

b) Windows 95

Versión del año 1995 que supone un gran avance con respecto a su precursor. Resuelve muchos de los antiguos problemas y se considera ya un sistema operativo dirigido totalmente al trabajo en red. En muchos aspectos se sitúa entre Windows 3.x y Windows NT. Como Windows 3.x trabaja con DOS y lo necesita para funcionar, pero su parecido con Windows NT es notable desde el punto de vista de cómo están programadas sus aplicaciones. Así programas escritos para Windows 95 se pueden ejecutar sin problemas en NT, pero no funcionan sobre 3.x.

Resumimos sus características:

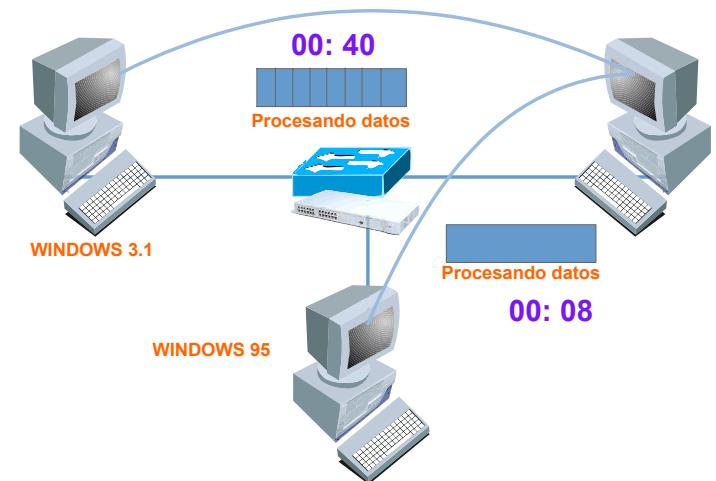
- Nueva interface, más cómoda y atractiva.
- Capacidad de conectar nuevo hardware y listo, lo que conocemos como “plug and play”.
- Windows 95 sigue ejecutándose por encima de DOS, necesitándolo, pero integrado hasta tal punto con éste que prácticamente se trata de un solo sistema operativo.
- Arquitectura del sistema de archivos a 32 bits. De todos los componentes nuevos que aparecen en Windows 95, el principal es el sistema de gestión de archivos, que ejecuta código de 32 bits en modo protegido de lectura y escritura en el sistema de archivos. Windows 95 todavía está influenciado por el código de 16 bits e incluso, Microsoft admite que Windows 95 no es un sistema operativo puro de 32 bits, de hecho, todavía tiene partes construidas sobre 16 bits. Sin embargo, el código a 32 bits es clave para las mejoras de velocidad del 95.

Nota:

FAT32 permite tamaños de unidades de asignación de 4 K. De esta manera se trabaja de manera más eficiente con los archivos de pequeño tamaño con respecto a FAT16, mejorando notablemente la “perdida” de espacio y soportando además discos de mayor tamaño (más de 2 Gigabytes).

c) Windows 98

Windows 98 es el sucesor de Windows 95 y se acerca todavía más a la plataforma Windows NT. La característica fundamental del 98 es su preparación para el trabajo en red, con soporte para mensajería, compartición de impresoras y archivos, explorador Web integrado con el sistema operativo, etc.



Anotaciones

Windows 98 es considerado junto con Windows Me como sistemas operativos de tipo “doméstico”, o sea construido para el trabajo en casa, facilitando una conexión a Internet fiable, así como mejores ofertas de ocio. Sin embargo el uso de Windows 98 en empresas de pequeño a mediano tamaño fue en su tiempo notable, y hoy día incluso encontramos el Windows 98 de manera habitual. Este éxito del 98 se basó en la mejora de su antecesor en puntos tan importantes como son:

- Fiabilidad.
- Comodidad en su uso, en su instalación y en su conservación.
- Mayor velocidad.
- Mayor integración con Web.

Windows 98 incluye todas las correcciones de errores encontradas por los programadores y usuarios durante tres años en su antecesor el 95, consiguiendo un sistema operativo con menores posibilidades de fallo. En caso de producirse estos fallos, siempre inevitables, Windows 98 mejora las utilidades de copia de seguridad y de recuperación de datos. Otro detalle importante con respecto a su fiabilidad es que con la versión 98 se pueden obtener actualizaciones del sistema operativo, parches que superan problemas encontrados, archivos con los últimos controladores, etc. Un proceso automático conecta al equipo con “Windows Update” dentro del sitio Web de Microsoft, obteniendo todos estos recursos.

El uso es más cómodo, con una interfaz de usuario cuya principal característica es la integración del Explorador de Windows con el Explorador Web, no sólo en su aspecto visual, sino fundamentalmente en su funcionamiento interno. Los usuarios todavía pueden usar la antigua interfaz heredada del 95 si lo desean, pero la nueva posee nuevas características como la ejecución de ciertas aplicaciones pulsando una sola vez el ratón, nuevos menús de herramientas, los botones de navegación Atrás / Adelante, etc.

Esta integración facilita la conectividad con Internet. Con Windows 98 el Explorer 4.0 se convierte en la interfaz de usuario unificada del sistema operativo. Anteriormente la conexión a Internet era un proceso muchas veces complicado y largo. Microsoft mejora el “Acceso telefónico a redes” y sobre todo, crea un “Asistente para la conexión a Internet”.

Windows 98 sigue dando soporte para los siguientes protocolos: NetBEUI, TCP/IP, IPX/SPX, DLC, etc. Sin embargo al ser TCP/IP el protocolo en el que se basan todas las comunicaciones de Internet, Windows 98 lo usa de manera predeterminada cuando se instala el sistema operativo y es el adecuado para el trabajo en Internet.

Anotaciones

Por supuesto NetBEUI sigue siendo utilizado, y se recomienda hacerlo si se trata de una red pequeña de varios ordenadores que tienen que compartir archivos e impresoras.

Una de las quejas más comunes del 95 era su lentitud al arrancar el sistema operativo, al apagarlo o al iniciar las aplicaciones. Windows 98 emplea varias técnicas para reducir el tiempo empleado en estas operaciones, cargando sólo los controladores que sean necesarios, eliminando la pausa de 2 segundos que tenía el 95 para pulsar F8 y entrar en el menú de arranque, y sobre todo cambiando el test automático de encendido o POST. Anteriormente este test automático de encendido procedía de la siguiente manera: Al encender el equipo se cuenta y examina la memoria, se giran los discos duros, se realizan varios diagnósticos, se inicia la memoria de video y se muestran los logotipos en pantalla, se comprueban las disqueteras y también el hardware “*Plug and Play*” y se comienza la carga del sistema operativo y de los controladores de dispositivos. Windows 98 posee un soporte que permite el retrasar algunas de estas operaciones e iniciarlas mientras el sistema operativo se está cargando o cuando esté ya cargado y sea el propio usuario el que las inicie a petición suya.

Como Windows 95, la arquitectura del sistema de archivos es a 32 bits. Windows 98 posee una arquitectura de red a 32 bits, con controladores de tarjetas de red a 32 bits, protocolos a 32 bits y aplicaciones a 32 bits para compartir archivos e impresoras.

d) Windows Me (Millennium Edition)

Después de la madurez conseguida con las versiones del 95 y 98, Microsoft lanza esta versión “Millennium” con una filosofía similar, o sea, dirigido principalmente al usuario doméstico. No es por tanto un sistema apropiado para el entorno profesional o de empresas, puesto que en ese momento, Microsoft apuesta por versiones más profesionales y robustas como Windows NT o Windows 2000.

Windows Me se basa en su facilidad de uso, con mejoras en la gestión y manejo del ordenador, en su funcionamiento de las redes de tipo domésticas, y en sus contenidos multimedia digitales.

Digamos que Me es la evolución del 95 y 98, y por lo tanto tiene el mismo núcleo, aunque presenta mejoras respecto a instalaciones de programas o drivers ajenos a Microsoft.

Definitivamente DOS desaparece, ya no se soportan aplicaciones DOS de 16 bits, no podemos reiniciar el sistema en modo MS-DOS, e incluso los archivos AUTOEXEC.BAT y CONFIG.SYS no poseen funcionalidad alguna. Los expertos sin embargo, comentan que DOS está por debajo de Windows Millennium todavía. De manera oculta, por supuesto. Lo que sí parece ser cierto es que la tendencia de los sistemas operativos basados en DOS termina con esta última versión Me.

Anotaciones

La apariencia es heredada de los sistemas 2000 y los iconos del escritorio son iguales que los de Windows 2000. El ícono "Entorno de Red" pasa ahora a llamarse "Mis sitios de red" y abarca ahora una estructura más amplia. Se mejora el Explorador de Windows en la vista rápida y "Mi PC" se simplifica y sólo muestra las unidades de disco y el "Panel de Control".

Quizás la mejora más notable de Me es en el terreno multimedia. La incorporación de Windows Media Player 7.0, un programa completo con multitud de recursos y accesorios, convierten a Windows Me en un sistema operativo muy apropiado para el uso doméstico y familiar.

Con respecto a las comunicaciones, Me lleva incorporado la versión 5.5 del Explorer, versión que ha resultado ser una de las más estables de Windows, y una utilidad de mensajería instantánea, el MSN Messenger. Con respecto al entorno red, sin embargo, Me no supone ningún adelanto sobre sus antecesores. Básicamente es idéntico a Windows 98.

Junto con la mejora en el entorno multimedia, Millennium incorpora dos nuevas utilidades de protección de datos:

- Sistema de recuperación de archivos (SFR), que trabaja de forma transparente al usuario e impide que programas o archivos defectuosos afecten a archivos esenciales del sistema.
- System Restore o Recuperación del Sistema. Básicamente almacena en el disco duro archivos que *nos recuerdan* la configuración del sistema. Si éste falla en un momento dado, se puede recuperar una configuración anterior. Estos archivos de configuración se guardan automáticamente al iniciar el equipo cada día, o antes de instalar un programa o en otro momento que hayamos programado, y aunque nos permite recuperar antiguas configuraciones y suele ser bastante útil, cada configuración ocupa bastante espacio en el disco duro.

e) Windows XP Professional.

Se trata de la última versión de sistema operativo Windows para estaciones cliente pero que ha adoptado la tecnología de NT y 2000 en cuanto al sistema de ficheros, la gestión de la memoria o la arquitectura de 32 bits. El kernel está protegido y puede desarrollar multitarea preferente con dos multiprocesadores.

Los cambios más visibles se pueden contemplar en su entorno de trabajo (novedoso y adaptable por los usuarios) y su capacidad para trabajar con medios ricos.

Anotaciones

Incorpora sistemas de seguridad y cifrado implementados en Windows 2000 y facilita mediante asistentes la conexión a entornos de red. Se trata de una versión que hace más sencillo el trabajo de cualquier usuario integrando asistentes para efectuar la mayoría de las tareas de configuración del equipo.

3.4. Redes en Windows.

a) Componentes de la red Windows.

- **Cliente:** es el que nos permite trabajar solicitando recursos de la red. Es él el que muestra la pantalla de *Inicio de sesión* al arrancar el ordenador, pidiendo la contraseña y el nombre de usuario.
- **Adaptador:** son las tarjetas de red que están instaladas en el ordenador. También está el *Adaptador de Acceso telefónico a redes*. En este caso, no hay una tarjeta de red, sino que el ordenador va conectado a un MODEM y éste a la línea telefónica.
- **Protocolos:** son los “lenguajes” que usa el ordenador para comunicarse. Normalmente se utiliza el protocolo **TCP/IP**, que es el que usa Internet, y el protocolo **NetBEUI**, para redes pequeñas.
- **Servicios:** los que ofrece Windows son *Compartir archivos e impresoras*.

b) Instalación de una red con Windows.

Las tareas que habrá que hacer en cada ordenador serán:

1. Instalar el adaptador de red. Tanto la instalación física como la lógica (drivers de la tarjeta de red).
2. Instalar Cliente para redes Microsoft.
3. Instalar protocolo/s (TCP/IP, NetBEUI).
4. Identificación, tanto del ordenador, como del Grupo de trabajo.
5. Instalar servicio *Compartir archivos e impresoras*.
6. Los ordenadores que, además, vayan a ofrecer algún archivo, carpeta o impresora, tendrán que configurar estos elementos como *compartidos* y decidir si lo hacen por medio de contraseñas y qué tipo de acceso quieren que tengan.

Anotaciones

c) Identificación del ordenador. Resolución de nombres.

A pesar de que un ordenador queda identificado por su IP, es mucho más cómodo en una red hacerlo por un *nombre*. Para esto, Windows identifica cada ordenador por “*Nombre de PC*” y “*Grupo de Trabajo*”, al que va a pertenecer el ordenador. Sin embargo, si usamos el protocolo TCP/IP, hay que traducir este nombre por su dirección IP.

Este proceso se conoce como “*resolución de nombres de dominio*”. Esto se puede hacer por varios métodos:

- *Broadcasting*: preguntando a todos los ordenadores de la red. Por defecto es este el método usado.
- *Archivo LMHOSTS*: contiene una lista que relaciona nombres con IPs.
- *Servidor WINS*: contiene una lista centralizada de IPs.

d) Compartir conexión a Internet. Acceso telefónico a redes.

Una situación muy típica en una pequeña red local, doméstica o pequeña oficina, es la de compartir una única conexión a Internet.

En esta situación, uno de los ordenadores de la red, llamado “*Equipo de conexión compartida*” o “*proxy*”, está conectado a Internet por medio de un *módem*, *adaptador RDSL*, etc.

Este ordenador es el único que tiene una IP pública y proporciona direcciones IP privadas y servicio de resolución de nombres a los restantes ordenadores de la red. El resto de ordenadores de la red tendrá acceso a Internet a través de él. Para Internet el único ordenador “visible” será este.

El ordenador proxy deberá tener instalado el adaptador virtual “*Acceso telefónico a redes*”. En esta situación, este ordenador se convierte en la puerta de salida al exterior de la red (*gateway*) y también en un *servidor DNS* (*nombres de dominio*) para esta red.

e) Conexión directa por cable.

Una situación muy simple, pero muy útil frecuentemente, es la de conectar dos ordenadores directamente, mediante un cable.

Windows contempla esta situación en su apartado de Comunicaciones.

En esta modalidad el primer ordenador hace de servidor del segundo y puede tener acceso a sus recursos, e incluso al grupo de trabajo del primero, a través de él.

Anotaciones

f) Compartición de archivos.

Una de las funciones de una red Windows, al igual que en cualquier red punto a punto, es la de distribuir los recursos entre todos los ordenadores de la red, y que, de este modo, puedan ser *compartidos* por todos.

Windows, permite compartir archivos, carpetas, directorios, unidades, etc. La decisión de compartir algo puede ser idea del grupo de trabajo, pero se debe hacer desde cada ordenador de la red. Un archivo se puede compartir como: Sólo lectura, Total o Dependiendo de contraseña en función de las distintas necesidades.

g) Compartición de impresoras.

Otro de los recursos que se puede compartir, son las impresoras. De este modo no es necesario tener una impresora para cada equipo y se puede tener una impresora mejor para todos.

Windows también contempla esto. Simplemente habrá que acceder a la impresora correspondiente y configurarla como compartida. De manera opcional podemos poner una contraseña de acceso.

h) Administración remota.

Es una herramienta para administrar una red Windows que puede resultar bastante útil. Consiste en poder administrar a distancia, desde un ordenador, otros ordenadores de la red.

Contempla dos casos:

- Si el equipo está configurado para el *control del acceso de los usuarios*, se podrá conceder a una persona o a un grupo permiso para usar los recursos que tenga compartidos en él.
- Si su equipo está configurado para el *control de acceso a los recursos*, se podrá conceder permiso para usar los recursos que tenga compartidos en él, usando la contraseña adecuada.

i) Seguridad.

Windows utiliza dos *contraseñas*:

- Contraseña Windows: para iniciar una sesión Windows.
- Contraseña de red Microsoft: para poder trabajar en red como clientes.

Anotaciones

Una vez que hemos dado estas contraseñas y estamos dentro de la red, tenemos dos opciones de control:

- Control de acceso a los recursos.
- Control de acceso a los usuarios.

En el apartado anterior vimos la compartición de recursos. Cada ordenador de la red puede compartir sus recursos, siempre que previamente tenga configurado este servicio en “Compartir archivos e impresoras”. Además, en cada recurso que comparta, puede controlar el tipo de acceso como: “Sólo lectura”, “Completo” o “Depende de contraseña”.

Si hemos elegido el *control* de acceso a usuarios, sólo tendrán acceso a los recursos los usuarios que estén permitidos.

En el “Acceso telefónico a redes” también existe una *contraseña* de conexión.

En Windows, varios usuarios pueden trabajar en un mismo ordenador, cada cual con su contraseña. Además se puede configurar el *perfil* de cada usuario. También existe una contraseña para la administración remota del ordenador, si se hubiera configurado así.

Windows tiene un editor de contraseñas para que estas puedan ser administradas.

Si la red tiene un ordenador proxy, se puede configurar éste para controlar el tráfico exterior de la red.

Las distintas versiones de estaciones cliente de Windows incorporan medidas de seguridad distintas. En Windows XP se añade el protocolo de seguridad Kerberos y la encriptación de archivos.

j) Monitor de red.

Es una utilidad de Windows que nos permite ver todos los recursos que el ordenador tiene compartidos y el tipo de acceso que se le ha asignado a cada recurso.

Podemos elegir la vista por:

- **Conexión:** usuarios que están conectados.
- **Por carpetas:** las que están compartidas y los usuarios conectados en ese momento.
- **Por archivos abiertos:** muestra los archivos usados por otros.

Se trata de una herramienta muy sencilla que permite testear la red. Las labores de administración que permite son muy básicas aunque necesarias en una red entre iguales.

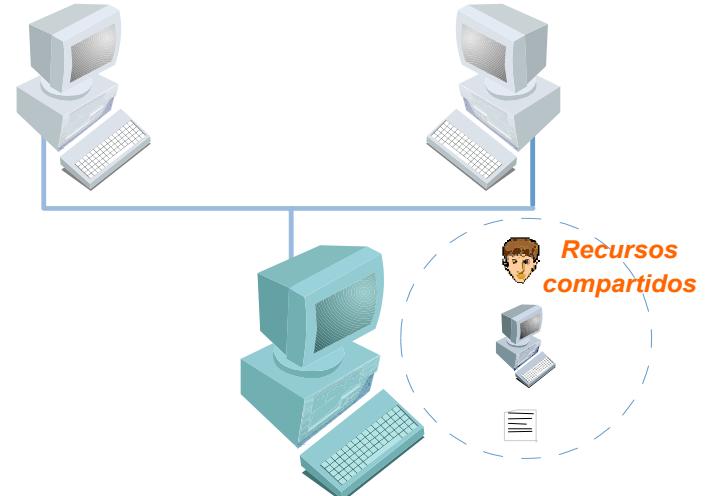


Ilustración 39: Monitor en red: Muestra el estado de los recursos que el ordenador tiene compartidos

Anotaciones

k) Conclusión.

Los distintos sistemas clientes de Windows proporcionan las funciones necesarias para trabajar en una red punto a punto, con una serie de aplicaciones para hacer la red operativa y eficaz. Con Windows XP, tendremos una red barata, fácil de instalar y administrar en la que podremos compartir archivos, carpetas, incluso impresoras.

Ventajas:

- Instalación de red barata, al ser una red entre iguales. El coste es muy superior en redes del tipo Cliente / Servidor.
- Facilidad de instalación.
- Administración fácil, no existe la imagen de un administrador dedicado.
- Mayor Integración con Web.
- Fiabilidad y velocidad ampliamente mejoradas.

Inconvenientes.

- *Inseguridad*: tiene pocos controles de seguridad, únicamente la contraseña Windows para el inicio de sesión y la contraseña de red para el trabajo en red como clientes.
- *Control*: no hay un control centralizado. El funcionamiento y comportamiento de la red depende del de cada uno de los ordenadores de ella. Son vitales los ordenadores que ofrecen servicios, como salida a Internet o de impresión, estén operativos en todo momento.
- *Tamaño*: estas redes son apropiadas para pocos ordenadores (menos de 10). No aguantan demasiado tráfico.
- *Instalación y configuración*: debe hacerse para cada equipo individualmente, así como las tareas de actualización.

Cuando incorporamos un equipo servidor podemos crear una red con control centralizado y con medidas de seguridad superiores. La creación de dominios y el uso de la herramienta Active Directory sólo se puede realizar con Sistemas operativos servidores. Mejora el control y se optimizan los recursos disponibles en la red, aunque requieren de conocimientos de administración avanzados. En un centro docente sería muy conveniente la utilización de este tipo de servidores pues la utilización de BDD con datos privados de alumnos, la gestión de expedientes económicos y académicos, etc. exigen la existencia de controles de seguridad estrictos para el acceso a los distintos recursos de la red.

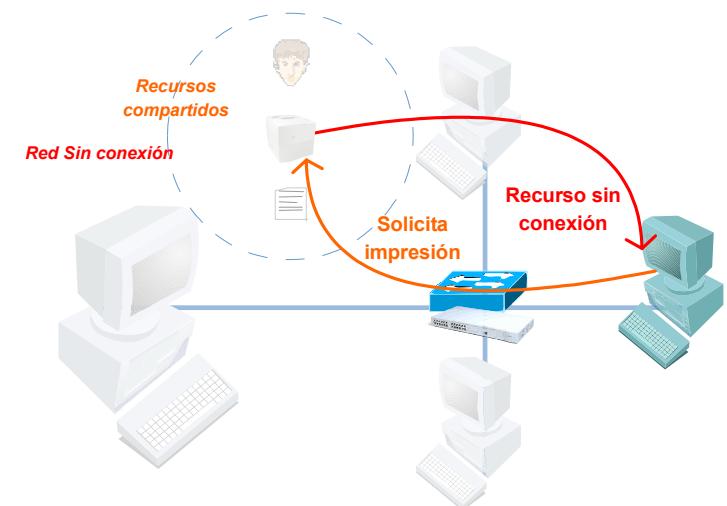


Ilustración 40: Red Windows: Una red Windows configurada como grupo de trabajo la configuración de cada PC condiciona el funcionamiento de la red

Anotaciones

3.5. Protocolos nativos de Windows.

No sería correcto afirmar que existen protocolos nativos de Windows, sin embargo, desde que se dieron los primeros pasos para crear sistemas operativos para trabajo en grupo, Microsoft optó por NetBEUI como protocolo predeterminado que proporcionaría servicios de transporte a NetBIOS.

NetBEUI dejó de ser el protocolo principal de Windows cuando se comprobó la eficacia e interoperatividad de TCP/IP y el tamaño de las redes comenzó a hacer patente las limitaciones de NetBEUI.

a) Protocolo NETBIOS.

Descripción general de NetBIOS.

NetBIOS (Sistema de Entrada Salida Básica de Red), es un protocolo estándar de IBM, que permite a las aplicaciones comunicarse dentro de una red de área local (LAN). Fue creado por IBM para una de sus primeras redes de área local (PC LAN) y posteriormente elegido por Microsoft como estándar para redes locales.

NetBIOS se puede implementar sobre una gran variedad de sistemas operativos de red, como: LAN Manager, LAN Server, Windows NT, Windows para trabajo en grupo, Windows 95/98, Lantastic, Banyan VINES, etc.

Este protocolo se diseñó para su uso dentro de grupos de PCs, que comparten un medio por difusión (broadcast). Proporciona dos tipos de servicio, con *conexión o sin conexión* y soporta broadcast y multicast.

La primera se conoce como *modo sesión* y funciona como el sistema telefónico, la conexión es como un tubo y los mensajes llegan en el orden en que fueron enviados. La segunda se conoce como *modo datagrama*, los mensajes son enviados de forma independiente como el sistema de correo y su encaminamiento es, igualmente, independiente.

Las aplicaciones NetBIOS emplean unos mecanismos propios para localizar recursos, establecer conexiones, enviar y recibir datos y cerrar la conexión. Todo esto se conoce como Servicios NetBIOS.

NetBIOS opera en la capa 5 (Sesión) del modelo OSI y, por tanto, proporciona los servicios de sesión de este nivel. Es un protocolo de aplicación para compartir *recursos en una red local*. Se encarga de establecer la sesión y mantener las conexiones.

Al operar en la capa 5 de OSI, no provee un formato de datos para la transmisión, tarea que es misión de otros protocolos. Los protocolos que pueden prestar el servicio de transporte a NetBIOS, pueden ser: IPX/SPX, NetBEUI o TCP/IP.

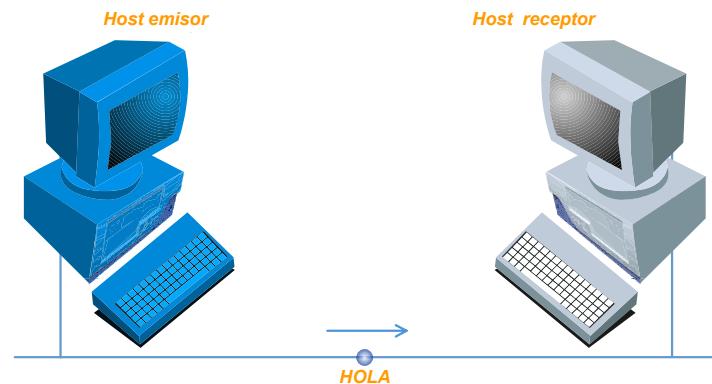


Ilustración 41: El modo sesión NetBIOS transmite los mensajes de forma ordenada llegando al host receptor organizados

Anotaciones

NetBIOS no se diseñó para una WAN (Wide Area Network), sino para LANs (Local Area Network), debido a esto es un protocolo de red no enrutable, que identifica a los equipos por un sistema de nombres no jerárquico, al contrario de como lo hace DNS. NetBIOS identifica a los ordenadores por su nombre; nombre de ordenador1, nombre de ordenador2, etc. Esta manera de identificar a los ordenadores por su nombre es bastante útil en una red pequeña, pero no en grandes redes.

Para pensar:

Cuando es necesario identificar un ordenador que pertenece a una red distinta a la que ocupa el equipo que decide comunicarse con él, es necesario dar dos niveles, al menos, de nombre, red y equipo. Sin embargo, si no encontramos en una red LAN, con un único dominio, todos los nombres se encuentran en la misma jerarquía, sólo necesitan un parámetro para definirlos.

Su característica de no enrutable, le hace funcionar encapsulando bajo TCP/IP, en lugar de crear un protocolo nuevo. De esta forma podemos trabajar en Internet. El uso de TCP/IP, principal protocolo de Internet, nos permite copiar archivos e imprimir documentos en cualquier lugar remoto, pero nuestro ordenador queda expuesto para ser atacado a través de Internet.

NetBIOS utiliza los puertos 137, 138 y 139. Hay fallos de seguridad en Windows debidos al protocolo NetBIOS. Por tanto, este protocolo se debe deshabilitar cuando no sea imprescindible. Es decir, en redes que disponen de otros protocolos que pueden realizar esas mismas funciones y que acceden a Internet.

El nombre que utiliza NetBIOS es el nombre que se pone, al iniciar Windows, en el cuadro "Nombre de PC", en la pestaña "Identificación" de las propiedades de Entorno de red.

Métodos de resolución de nombres NetBIOS.

Hay varios métodos:

- **Caché NetBIOS:** En cada ordenador hay almacenada una tabla dinámica que contiene los últimos nombres de los otros ordenadores de la red. Esta tabla se puede obtener con el comando `nbtstat -r`.
- **Broadcasting:** Se pregunta el nombre a todos los ordenadores de la red.
- **Archivo LMHOSTS:** Es un archivo de texto, que tiene cada ordenador de la red, con una lista de direcciones IP y nombres NetBIOS.

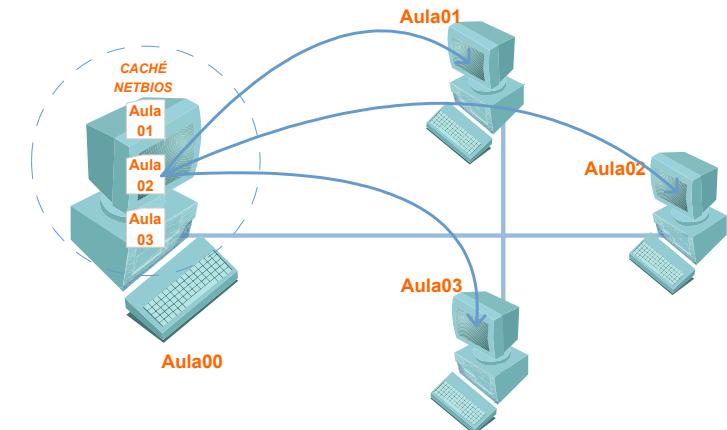


Ilustración 42: CHACHÉ NETBIOS: Almacena los nombres en una tabla dinámica

Anotaciones

- **Servidor WINS:** Es un ordenador con una tabla con las direcciones IP y nombres NetBIOS. Esta tabla se crea y modifica dinámicamente, a medida que se van conectando y desconectando ordenadores en la red. Este es el método más recomendable para redes medianas y grandes. El servidor puede ir con Windows NT o 2000. Cada vez que se escribe un nombre, se consulta al servidor WINS.

El método que se emplea para determinar las direcciones de equipo utiliza, más frecuentemente, dos técnicas, broadcasting y tablas LMHOST. Antes de enviar un mensaje de broadcasting, que genera mucho tráfico en la red, se consulta una tabla, que relacione los nombres NetBIOS con sus correspondientes direcciones IP. Esta tabla se guarda en un archivo llamado LMHOSTS. Windows consultará el archivo LMHOSTS antes de hacer un broadcasting a la red.

Además de la resolución de nombres, NetBIOS es responsable de las siguientes funciones:

- **Servicio de datagramas NetBIOS** es un servicio que permite enviar mensajes a distintos equipos o grupos de una red. No garantiza que dichos mensajes lleguen.
- **Servicio de sesión NetBIOS** que permite abrir una conexión punto a punto entre dos equipos de una misma red.
- **Estado de sesión/NIC NetBIOS** cuya tarea fundamental es ofrecer información sobre las NIC de una red y las sesiones que hay establecidas.

b) Protocolo NetBEUI.

NetBEUI (Interfaz de Usuarios Extendida NetBIOS), es como su nombre indica una versión *extendida* de NetBIOS. En Microsoft se le conoce también como NBF.

En el manual de recursos de Microsoft Windows para Grupos, se encuentra la siguiente definición: “*el protocolo primario usado en Windows para Grupos es llamado NetBEUI (NetBIOS Extended User Interface). Este protocolo fue introducido por IBM en 1985. NetBEUI es un protocolo pequeño y eficiente diseñado para su uso en una red LAN departamental de 20 a 200 estaciones de trabajo.*”

Sus características básicas son:

- No enrutable puesto que emplea el espacio de nombres de NetBIOS que no posee mecanismos para identificar redes.
- Se diseñó para redes LAN, emplea en la mayoría de los casos transmisiones de difusión y no es enrutable (tal como ya hemos indicado)

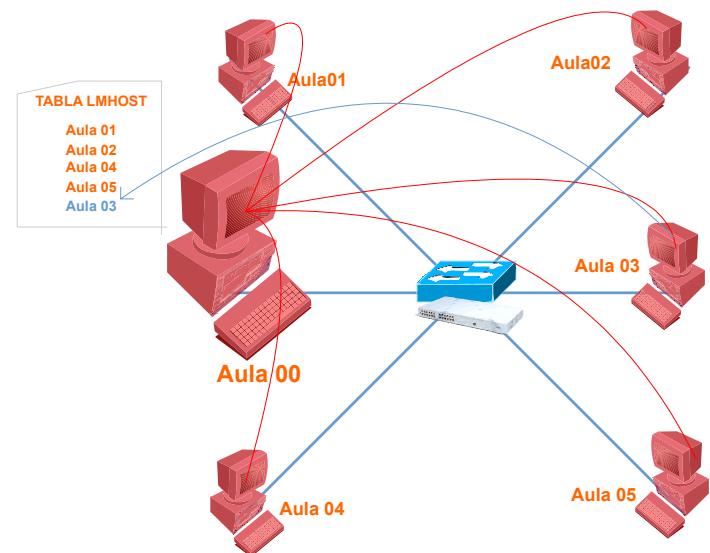


Ilustración 43: Tabla LMHOST: Antes de realizar BROADCAST el host analiza su tabla LMHOST, si no encuentra el nombre, lo solicita a la red

Anotaciones

- Necesita ser encapsulado en TCP/IP

En un segmento de red local, NetBEUI es el protocolo más rápido de los suministrados con Windows, sin embargo no es un protocolo diseñado para redes WAN ni para ningún tipo de red compuesta de más de un segmento.

Se trata más bien de un protocolo para redes LAN de Windows que es muy efectivo como protocolo principal y que puede ser acompañado por otros secundarios en función de las necesidades del sistema.

c) Relaciones NetBIOS/ NetBEUI / TCP/IP

Puesto que NetBEUI es muy rápido para comunicaciones dentro de redes locales de pequeño tamaño es recomendable, al configurar una red, implementar NetBEUI en cada una de los ordenadores que necesiten acceder a otros a través en una red LAN. La tecnología de Windows para redes está basada en NetBIOS y NetBEUI. NetBEUI provee los servicios de transporte de datos contemplados en las capas 3 (Red) y 4 (Transporte) del modelo OSI.

El inconveniente que posee este protocolo es que no es enrutable. Esto significa que no sirve para trabajar en redes WAN (Redes de Área Media). En estos casos, se recomienda instalar NetBEUI y TCP/IP. El primero se usaría para las comunicaciones dentro de la LAN y TCP/IP para las comunicaciones hacia afuera de la LAN.

Analogía:

NetBEUI emplea la interfaz NetBIOS como una interfaz de nivel superior y NetBIOS usa NetBEUI para el transporte de datos. En un símil de transporte, NetBIOS sería el pasajero que será transportado por dos tipos de transporte NetBEUI o TCP/IP. El primero para las distancias cortas y el segundo para las largas.

Las redes, cuyos ordenadores llevan el sistema operativo Windows, utilizan para comunicarse entre sí el protocolo NetBIOS. Este protocolo, a su vez, debe ir sobre otro de nivel inferior que puede ser uno de los siguientes: NetBEUI, IPX/SPX, TCP/IP. Debido a esto se habla de NetBIOS sobre TCP/IP o NetBIOS sobre NetBEUI.

TCP/IP usa números para representar las direcciones de los ordenadores, mientras que NetBIOS usa nombres. Este fue el mayor problema que hubo que solucionar para que se relacionasen los dos protocolos. En 1987, El IETF (Internet Engineering Task Force), publicó una serie de documentos de estandarización (los RFC 1001 y 1002), que explican cómo NetBIOS puede trabajar sobre una red TCP/UDP.

Anotaciones

4. Redes Linux.

4.1. Introducción.

Hablar de redes de ordenadores a menudo significa hablar de UNIX. Creado en los 70 por un grupo de programadores en los laboratorios Bell como un sistema operativo multiusuario y multitarea, pequeño y flexible, UNIX es uno de los más populares del mundo debido a su extenso soporte y distribución. Según muchos programadores, UNIX es el auténtico y único sistema operativo: Robusto, eficaz y versátil. Es uno de los primeros sistemas operativos creados en el lenguaje de programación de alto nivel C. Esto hace posible su instalación en cualquier máquina que tenga un compilador de C.

UNIX es el sistema operativo más extendido en equipos servidores. Se trata de un sistema de propósito general, tal como se ha adelantado en la introducción de este capítulo, con características de multiusuario y multitarea.

Existen dos versiones de UNIX, Solaris y Linux. Optaremos por analizar más detenidamente esta última por sus características de desarrollo y su mayor extensión en el mundo educativo.

a) Breve historia de linux.

Linux es un sistema operativo para PCs basados en Intel, que intenta ser un clon de UNIX, sin ningún software comercial con derechos de autor y que pueda utilizar todo el mundo. Comenzó como una afición de Linus Tovarls mientras estudiaba en la universidad de Helsinki. Su objetivo era crear un sustituto de Minix, similar a UNIX. Poco a poco, y a través de Internet, muchos internautas ofrecieron su ayuda a Linus, reportando fallos en el núcleo del sistema (Kernel), mejorando el código y añadiendo controladores. Así, llegamos al estado actual donde la última versión estable del kernel Linux alcanza unos niveles de estabilidad, escalabilidad y rendimiento que Linux no podría ni imaginar cuando empezó su proyecto en 1991.

Linux nació ya, como sistema operativo para trabajo en red, de manera que muchos de los problemas que otros sistemas operativos tuvieron que solucionar sobre la marcha a lo largo de su evolución, los desarrolladores de Linux ya los contemplaban. Así, Linux es un sistema operativo sobre el que se pueden montar estaciones clientes y servidores, sin más que implementar los servicios necesarios (Web, FTP, DHCP, etc.) en cualquier estación. Es decir, no es necesario emplear un sistema operativo servidor, sino añadir servicios a cualquier estación.

Anotaciones

En un principio, Linux era un núcleo al que se podían incorporar una serie de aplicaciones obtenidas a través de Internet. Posteriormente, según iba evolucionando como sistema operativo y adquiriendo notoriedad, se comenzaron a desarrollar distribuciones del sistema operativo con distintas aplicaciones e interfaces de instalación. Estas distribuciones han evolucionado hasta nuestros días diferenciándose progresivamente, por lo que podríamos hablar de distintas versiones/distribuciones de Linux.

b) El concepto de software libre.

El movimiento GNU/ Linux tiene de trasfondo el concepto de “*software libre*”. Se desarrolla bajo las reglas del proyecto de GNU de Free Software Foundation, Cambridge, Massachusetts y básicamente significa que los usuarios tienen libertad de ejecutar, copiar, distribuir, instalar, cambiar y mejorar el programa tantas veces como quieran. En concreto se consideran tres niveles de libertad:

- Libertad para estudiar el programa, aprender de él e incluso usar todo o parte en otros proyectos.
- Libertad para distribuir, copiar a quien se quiera y sin límite alguno; cobrándose por ello lo que se quiera.
- La Libertad de toda la comunidad de usuarios de mejorar el programa y distribuirlo de tal manera que se puedan beneficiar todos los integrantes de la propia comunidad.

Con el software libre, la única libertad que no se tiene es la de restringir estos derechos a otros usuarios, es decir, la libertad de eliminar libertades. Si se distribuye una copia o una modificación de un programa libre todos los usuarios tienen los derechos antes citados.

4.2. Características del Sistema Operativo Linux.

Linux es un sistema operativo completo multitarea y multiusuario. Esto significa que pueden trabajar varios usuarios simultáneamente en él, y que cada uno de ellos puede tener varios programas en ejecución. Lo explicamos detalladamente a continuación:

- **Multiusuario:** varios usuarios pueden acceder a las aplicaciones de un único PC. La característica que más resalta de Linux es que un grupo de personas puede trabajar con la misma versión de la misma aplicación al mismo tiempo, desde el mismo terminal o desde terminales distintos.

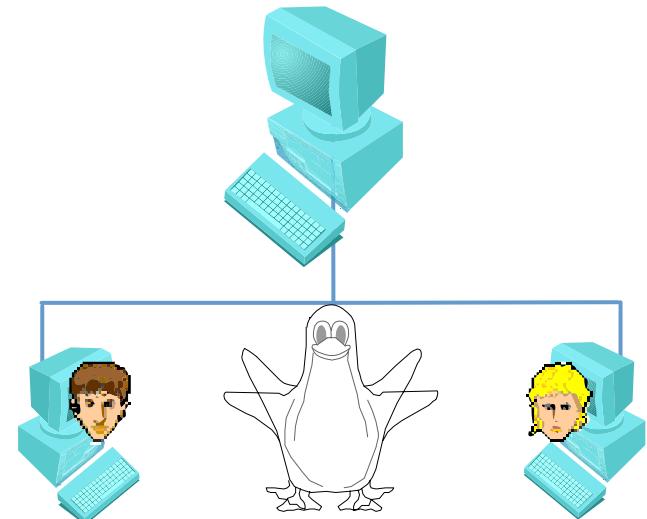


Ilustración 44: Linux: Es un sistema Operativo multiusuario

Anotaciones

- **Multitarea:** describe la capacidad de ejecutar muchos programas al mismo tiempo sin detener la ejecución de cada aplicación. Linux se basa en la *multitarea prioritaria* donde cada programa tiene garantizada la oportunidad de ejecutarse, y se ejecuta hasta que el sistema operativo da prioridad a otro programa para ejecutarse. MS-DOS y Windows 3.1, por ejemplo, se basan en una forma de multitarea denominada *multitarea cooperativa*. Con ésta, los programas se ejecutan hasta que permiten voluntariamente que se ejecuten otros programas o no cesan su actividad por el momento. En Linux, el microprocesador sólo es capaz de hacer una tarea a la vez, pero las realiza en tiempos tan cortos que no los notamos y es en sus "ratos libres" donde se dedica a ejecutar otras tareas que se le hayan pedido.

Además de estas propiedades, Linux se caracteriza por:

- **Multiplataforma:** corre en muchas CPUs distintas, no sólo Intel.
- **Protección de la memoria entre procesos,** de manera que uno de ellos no pueda colgar el sistema.
- **Carga de ejecutables por demanda:** Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.
- **Política de copia en escritura** para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- La **memoria** se gestiona como un recurso unificado para los programas de usuario y para la caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta puede a su vez ser reducida cuando se ejecuten grandes programas.
- **Consolas virtuales múltiples:** podemos entrar como diferentes usuarios de la máquina o como el mismo usuario y trabajar en distintas consolas virtuales. Es como si en el mismo ordenador tuviéramos varias terminales.
- **Soporta TCP/IP**, incluyendo ftp, telnet, NFS, etc.
- **Software cliente y servidor Netware** disponible en los núcleos de desarrollo.

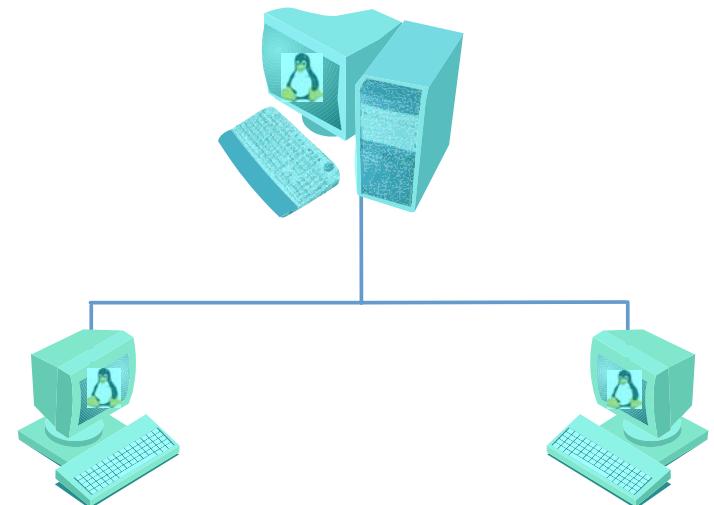


Ilustración 45: Consolas virtuales múltiples Linux admite varias consolas virtuales

Anotaciones

4.3. Sistema de archivos de Linux.

Linux es un sistema operativo que está estructurado en archivos. Todos los elementos de hardware o software de un equipo están gestionados a través de un archivo. El sistema Linux es una estructura de directorios jerárquica donde se organizan los archivos. Posee una estructura de árbol donde la parte superior es su raíz. Este sistema permite ubicar cualquier dispositivo dentro de la estructura de archivos, aunque se encuentre en otra unidad de red.

Para pensar:

MS-DOS empleaba también un sistema e archivos similar, la principal diferencia radica en que la estructura de archivos de DOS se realizaba a partir de unidades físicas, DISCOS, mientras que en Linux los discos se encuentran como directorios dentro de la propia estructura de árbol, se sigue más bien, una organización lógica.

El árbol de directorios suele contener una serie de directorios que incluyen otros subdirectorios, son pues sistemas de archivos incluidos en otros sistemas más amplios. Esta característica tiene como consecuencia que el nombre de un archivo no sea el nombre que se le ha asignado al crearlo, sino la ruta de ese archivo en el árbol de directorios añadiéndole, al final, su nombre.

Analogía:

El sistema de archivos de Linux asemeja, como ya hemos indicado, a un árbol, más bien un arbusto, de cuya raíz crecen todas las ramas. Estas ramas serían los directorios, de cada rama pueden crecer más ramas (subdirectorios) o salir hojas (archivos).

Los directorios presentes dentro del sistema raíz suelen ser:

- **/bin:** contiene los programas ejecutables binarios.
- **/sbin:** archivos binarios de sistema orientados a su administración.
- **/etc:** incluye gran parte de los archivos de configuración del sistema.
- **/lib:** contiene las bibliotecas de opciones compartidas de los distintos programas.
- **/dev:** contiene los archivos de dispositivo que son empleados para acceder a los elementos de hardware.

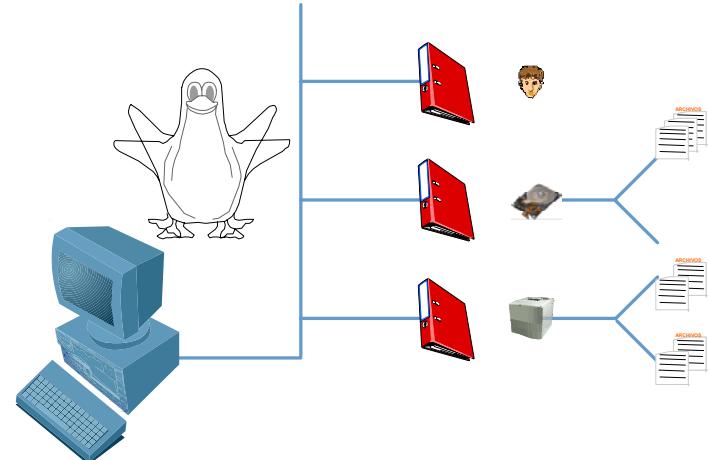


Ilustración 46: Árbol directorio de Linux: Es una estructura jerárquica

Anotaciones

Capítulo 5: Sistemas operativos de red

- **/proc:** incluye los procesos que se están ejecutando en ese momento por el sistema.
- **/tmp:** almacena los archivos temporales.
- **/home:** se emplea para guardar los directorios de los usuarios de los equipos.
- **/var:** incluye los archivos que pueden modificar su tamaño.
- **/usr:** contiene todos los archivos y órdenes usados por el sistema. Este directorio se divide en otros subdirectorios.
 - **/usr/bin:** órdenes orientadas a los usuarios y programas de utilidades.
 - **/usr/sbin:** órdenes de administración de sistemas.
 - **/usr/lib:** incluye las bibliotecas de los lenguajes de programación.
 - **/usr/doc:** incluye los documentos de Linux.
 - **/usr/man:** archivos del manual interactivo.
 - **/usr/spool:** contiene los archivos en formato spool.

Un aspecto que indica cómo Linux desde un principio es un sistema multiusuario es la presencia de la carpeta home, en la que se incluyen todos los usuarios que están creados en ese sistema.

Por otro lado, Linux ha creado una estructura lógica que permite aprovechar cualquier sistema de ficheros, FAT 16, FAT 32, etc. y montar, además particiones Linux nativa o ext. Cada directorio debe incluir las entradas de cada archivo que contiene. Es decir, aunque parezca que los archivos se encuentran dentro de una carpeta, físicamente no es así, los archivos se encuentran distribuidos por el disco, pero están asociados a otro archivo (directorio) que incluye la información (entradas) para poder localizarlos.

Para poder acceder a cualquier archivo es necesario que el sistema averigüe cuáles son los bloques de datos del disco en los que este archivo está grabado. Por cada archivo, su directorio almacena una cadena de datos que forman el nombre del archivo (ruta) y un número. El número indica cuál es la estructura de datos que contiene la información de ese archivo; esta estructura de datos se conoce como inodo, un inodo por cada archivo. Es el inodo del archivo el que contiene, entre otras, la información sobre los bloques de datos en los que se encuentra ubicado cada archivo.

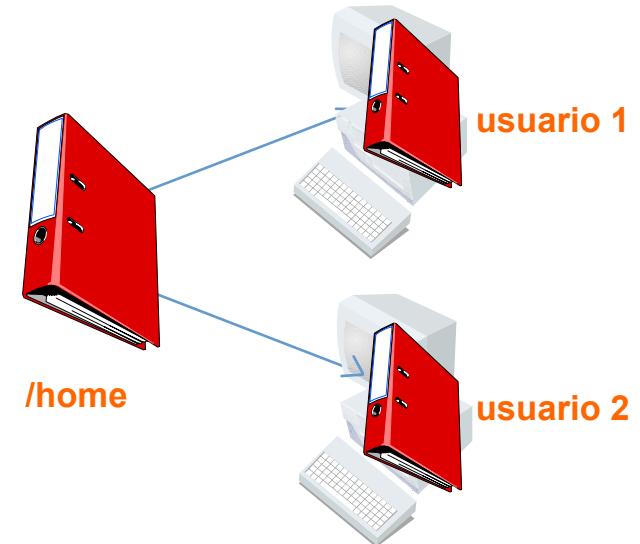


Ilustración 47: Carpeta/home: Almacena los archivos de cada usuario

Anotaciones

4.4. Montaje de dispositivos.

Linux maneja los dispositivos de almacenamiento como un archivo más dentro del directorio raíz.

Cuando realizamos una nueva partición, deberemos establecer un punto de montaje para dicha partición, es decir, una carpeta en la que ubicar el dispositivo que vamos a crear. El sistema que emplea Linux para las particiones de los discos es similar al de DOS. Sin embargo, mientras que DOS asigna a cada partición una letra D, E, etc., el sistema de Linux no.

Nota:

Cuando montamos una distribución de Linux es conveniente realizar, al menos, dos particiones, la primera para ubicar el sistema operativo, con cualquier sistema de ficheros Linux y la segunda swap (intercambio) para emplearla como almacenamiento cuando la memoria se encuentre llena y necesite depositar esos procesos en el disco duro.

Los discos duros se identifican mediante letras hda, hdb y cada una de las particiones de un disco mediante números hda1, hda2, etc.

Una vez que hemos formateado la unidad (creado el sistema de ficheros) debemos montarla para que pueda ser utilizada por el sistema. Es decir, debemos indicar qué directorio y qué nombre vamos a asignarle, este proceso, tal como hemos indicado, se denomina montaje. La ventaja de este proceso consiste en su flexibilidad, puesto que una vez que hemos montado un disco o una partición como carpeta dentro del sistema de archivos, podemos trabajar con ella como otro directorio más, es decir, podemos copiarla, moverla, etc. como si se tratara de un archivo de texto.

Del mismo modo que montamos una partición en nuestro árbol de archivos, podemos montar una unidad de red, es decir, incorporar a nuestro directorio una carpeta compartida por otro equipo de la red y manejárla como si estuviera en local de forma completamente transparente.

Cualquier dispositivo de almacenamiento debe ser montado en el árbol de archivos. Sin embargo, la partición en la que se ha instalado el sistema operativo aparecerá como raíz y no se le aplica el proceso que acabamos de explicar.

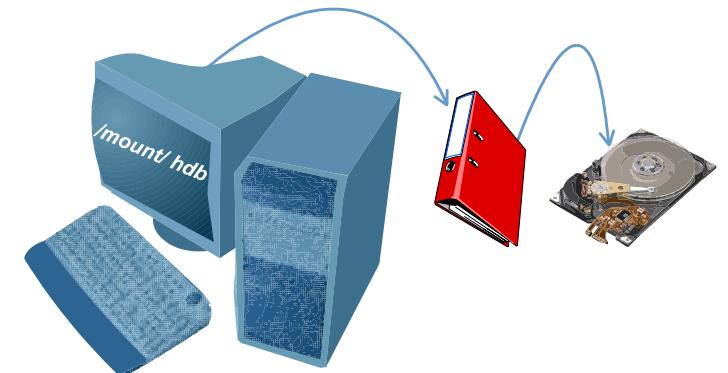


Ilustración 48: Montaje de dispositivos: Cualquier dispositivo de un PC debe ser montado como un archivo para poder ser utilizado

Anotaciones

4.5. Aspectos generales.

a) Intérpretes de comandos “shell”.

Un intérprete de comandos no es sino un programa que lee instrucciones del usuario a través del teclado y las ejecuta. Existen multitud de intérpretes de comandos, pero los más usados son **tcsh** (especialmente en UNIXs comerciales) y **bash**, que se puede decir es el estándar en los sistemas Linux.

El intérprete de comandos le indicará al sistema que está esperando instrucciones mostrando lo que se denomina el *prompt* del sistema. Puede mostrarse de formas diferentes, puesto que es configurable por el usuario, pero generalmente será un símbolo \$ o #, dependiendo si se trata de un usuario normal o del usuario root.

Al pulsar *intro*, se le indicará al sistema que ha acabado de introducir el comando. Entonces hace varias cosas con él. Primero comprueba si el comando es interno al intérprete de comandos y si puede ejecutarlo por si mismo.

También comprueba si el comando es un alias, o un sustituto de nombre de otro comando. Si no cumple ninguna de estas dos condiciones, el intérprete de comandos busca un programa que tenga el nombre especificado. Si tiene éxito el intérprete ejecuta el programa, mandándole los argumentos especificados en la línea de comandos.

b) Entorno gráfico.

El sistema Xwindow.

Xwindow fue desarrollado a mediados de los 80 como respuesta a la necesidad de un interfaz gráfico transparente para los sistemas UNIX. Es el encargado de visualizar la información de manera gráfica, y es totalmente independiente del sistema operativo, el cual puede ser trabajado totalmente en modo texto.

La diferencia entre Xwindow y otros interfaces gráficos es que Xwindow establece un enlace cliente-servidor: el cliente X especifica el “qué hacer” al servidor X, que se encargará de “Cómo hacerlo”. El servidor X de una aplicación y el cliente X no tienen porque estar en la misma máquina. Podemos utilizar Xwindow en nuestra máquina, conectarnos a otra remota, ejecutar un programa en la remota y visualizarlo en nuestra máquina local. Esto es totalmente independiente de la plataforma/ sistema operativo que la máquina remota utilice.

Existen distintas versiones de Xwindow: comerciales y bajo licencia GNU. De estos últimos es de destacar Xfree86, incluido en todas las distribuciones Linux.

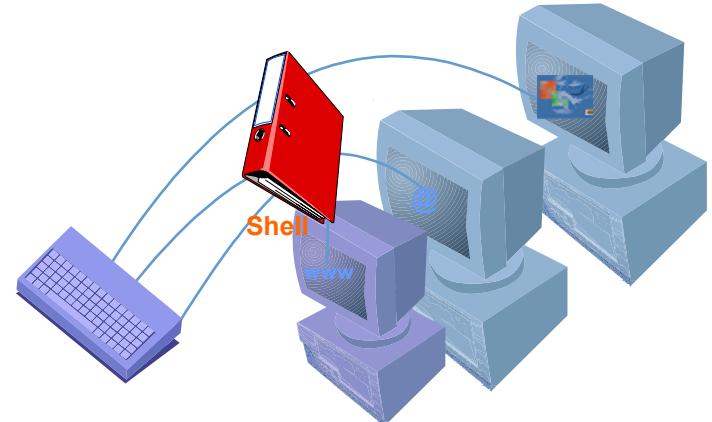


Ilustración 49: Shell: Es un intérprete de órdenes para que el usuario interactúe con el sistema

Anotaciones

Gestores de ventanas.

Un gestor de ventanas es el conjunto de programas, ventanas, funcionalidades..., que hacen posible que el usuario pueda interactuar con el sistema de forma gráfica y no en modo texto. Lo podríamos comparar al entorno gráfico que todos conocemos de Windows. Esta basado en el motor gráfico Xfree86 y existen numerosos y variados tipos, unos más desarrollados y estables que otros. Es el usuario el que tiene que decidir cual es el que le conviene, pudiendo tener instalados varios. Evidentemente es totalmente independiente del sistema operativo, y muchos usuarios trabajan en modo texto sin ningún problema. Algunos de los gestores de ventanas más populares son: Gnome, KDE, icewm, FVWM, Window Maker, Enlightenment...etc.

c) Usuarios y grupos.

Para acceder a una máquina Linux es necesario identificarse como usuario. Este proceso de identificación permite al administrador flexibilizar al máximo la utilización de los recursos de la red, puesto que se puede determinar quién o quiénes pueden o no pueden acceder a cada uno de los archivos que se encuentran en el sistema, y de qué forma pueden hacerlo.

Nota:

No debemos olvidar que cualquier elemento de una red o un equipo es un archivo o un directorio dentro del árbol de directorios de Linux. Si restringimos la lectura, escritura, etc. a un grupo de usuarios en un archivo, podemos estar impidiendo su ejecución.

Igualmente, si permitimos esos procesos a un grupo o un usuario, le asignamos un control total sobre ese elemento.

Disponer de este sistema exige la utilización de un método que permita distinguir unos usuarios de otros, debe tener, pues, cada usuario, una identificación única. Además, a cada usuario se le asocia un directorio propio en el que guardar sus archivos. Este directorio se puede montar en una máquina local o en un servidor remoto. Por último, es necesario que, asociada a cada cuenta de usuario exista una contraseña, conocida únicamente por este, que evite que otros usuarios accedan a su información. Un usuario es aquel que dispone de una cuenta en el sistema en la que se recogen los datos asociados a un mismo usuario.

Un grupo de usuarios es, básicamente, una organización administrativa. Se emplea para facilitar la gestión de los mismos en función de parámetros de administración más generales. Un usuario puede pertenecer a varios grupos, pero también puede actuar de forma independiente en el sistema.

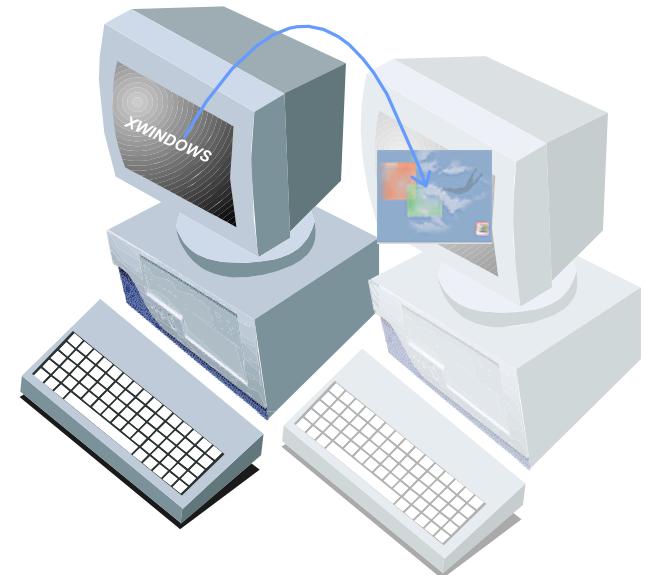


Ilustración 50: Gestor de ventanas: Permite interactuar en forma gráfica

Anotaciones

Capítulo 5: Sistemas operativos de red

Los elementos que caracterizan a un usuario son:

- a) **Nombre de usuario:** es el identificador del usuario dentro del sistema. Debe ser un identificador único.
- b) **Nombre real:** Nombre real del usuario.

Nota:

El nombre de usuario también es conocido como login Es decir log in. Acceso al sistema.

- c) **Contraseña:** Serie de caracteres que permiten confirmar la identidad de un usuario. Las contraseñas no aparecen en pantalla y deben ser encriptadas para que no puedan ser desveladas. El administrador puede obligar a los usuarios a que cambien de contraseña cada cierto tiempo.
- d) **Directorio de entrada (directorio home):** Es un directorio propio donde cada usuario puede almacenar sus ficheros. Este directorio se crea automáticamente al crear un usuario en la carpeta /home añadiendo la carpeta propia de ese usuario con su nombre /home/usuario; el administrador puede determinar el lugar en el que se creará la carpeta.

Para pensar:

La carpeta home puede ser una unidad compartida de un servidor de archivos que se monta en local cada vez que accede al sistema un usuario.

- e) **Identificador numérico:** Identificador numérico de cada usuario.
- f) **Shell:** Cuando un usuario accede al sistema se le asigna un shell o sistema de comandos para interactuar con la máquina.
- g) **Grupo de entrada:** Es el grupo prioritario que se asigna al usuario cuando accede al sistema.
- h) **Grupos adicionales:** Otros grupos a los que pertenece el usuario.
- i) **Caducidad de la cuenta:** Posibilita el que un usuario sólo pueda acceder al sistema hasta un momento determinado.

Todas estas opciones son configurables cuando el administrador crea un usuario.

Anotaciones

Del mismo modo que existen una serie de atributos de usuario, podemos indicar algunos elementos que caracterizan a los grupos. Estos son:

- a) Nombre del grupo.
- b) Identificador numérico del grupo.
- c) Nombres de los usuarios miembros del grupo.
- d) Contraseña del grupo.

La cuenta root.

Linux distingue diferentes rangos de usuarios. Cada usuario recibe una cuenta que incluye un nombre de usuario y un directorio inicial, entre otras cosas. Además de las cuentas dadas a personas reales, existe otra, definida por el sistema, con privilegios especiales: la cuenta raíz, con el nombre de usuario root.

Los usuarios normales están restringidos para que no puedan dañar o borrar ficheros vitales del sistema. Si se comete un error, éste sólo afectará a su cuenta. Estas restricciones desaparecen para el usuario root, que puede leer, modificar o borrar cualquier fichero en el sistema, cambiar permisos y pertenencias en cualquier fichero y ejecutar programas especiales, como pueden ser los que partitionan un disco o crean sistemas de ficheros.

Para pensar:

Puesto que root puede hacer todo, es fácil cometer errores que tengan consecuencias catastróficas cuando se trabaja utilizando esta cuenta. Es conveniente seguir estas precauciones:

- *Pensar dos veces antes de presionar <enter> en un comando que pueda causar daño.*
- *No acostumbrarse a utilizar la cuenta root, y si es necesario hacerlo, desconectarse en el momento en que terminemos de trabajar con ella.*
- *El root debe disponer de una cuenta de usuario que permita realizar operaciones habituales sin correr el riesgo de dañar gravemente el sistema.*

Las redes Linux disponen de un sistema de administración muy fuerte. Desde el comienzo de la instalación de un equipo o la creación de un usuario se necesita de la intervención del administrador que será, al fin y al cabo será quien defina hasta el último detalle la configuración de la red.

Anotaciones

4.6. Administración.

Linux no dispone de una base de datos centralizada en la que se recojan todos los recursos existentes en la red, similar a Active Directory o Novell Directory Services. Su sistema de ficheros y la estructura jerárquica de sus directorios permite realizar alguna de las tareas de estas herramientas, sin embargo, el peso de la administración de una red Linux depende, fundamentalmente, de la capacidad del administrador y de cómo halla planificado el montaje y crecimiento de su red.

a) Sistemas de permisos. Administración de archivos.

Administración de archivos.

Cualquier archivo que se encuentre en un sistema Linux tiene asignada una serie de características. Una de ellas es los permisos de acceso. En este sentido, Linux establece dos niveles. En primer lugar determina quiénes pueden acceder y en segundo lugar, en qué condiciones. Con respecto a quiénes pueden acceder determina tres grupos:

- El usuario propietario del archivo.
- El grupo al que pertenece.
- Todos los usuarios del sistema.

Por otro lado, cada uno de estos posibles usuarios que deseen acceder al archivo, pueden tener varios permisos dentro de dicho archivo:

- Lectura.
- Escritura.
- Ejecución.

Cualquiera de estos permisos pueden ser atribuidos a cualquiera de los usuarios que hemos descrito anteriormente.

Para pensar:

Un archivo de texto puede tener permiso de ejecución, aunque parezca absurdo. Es evidente que, aunque un usuario tenga permiso para ejecutar uno de estos archivos, no podrá debido a que no son ejecutables.

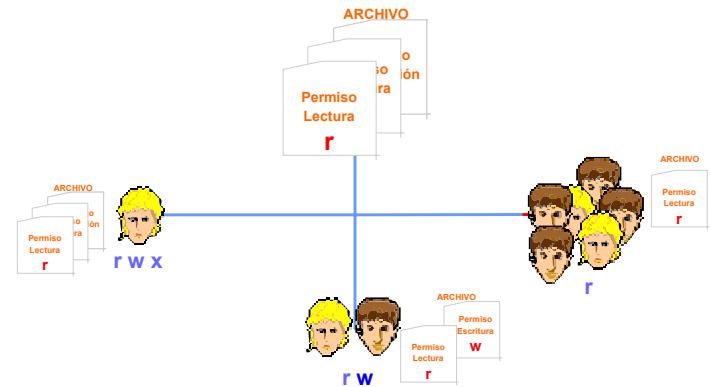


Ilustración 51: Sistema de Permisos en Linux: Un archivo tiene asignados permisos de lectura, escritura y acceso a su propietario, grupo al que pertenece y todos los usuarios

Anotaciones

Administración de directorios.

Al igual que los archivos, los directorios también disponen de permisos. La gestión de los usuarios es similar a la del sistema anterior, sin embargo, los permisos varían en los siguientes aspectos:

- Lectura: permite visualizar los archivos que incluye.
- Escritura: permite crear y suprimir archivos en el directorio.
- Ejecución: permite el desplazamiento a dicho directorio.

Si un usuario no tiene permiso de acceso a un directorio, no podrá acceder a un archivo que esté incluido en el mismo, aunque tenga permiso para ello.

b) Compartición de recursos.

Linux permite compartir recursos en toda la red. Para ello emplea distintos sistemas, pero, el objetivo final es disponer de un sistema de archivos distribuidos totalmente transparente para el usuario. Estos sistemas implementan procedimientos cliente-servidor y deben permitir una compartición de recursos sencilla basada en los siguientes principios:

- Transparencia de red: los ficheros remotos aparecen como locales.
- Independencia de posición: el nombre del fichero no debe cambiar aun cuando cambie su ubicación.
- Movilidad de usuarios: el acceso a los recursos compartidos debe ser independiente del nodo desde el que se acceda.
- Tolerancia a fallos.
- Escalabilidad: el sistema debe poder adaptarse a un crecimiento de carga y de estructura.
- Movilidad física de los ficheros.

La opción por uno u otro sistema dependerá del modo en el que trabajen cada una de las características descritas y de la facilidad de administración que ofrezcan. La implantación de cada uno de estos sistemas está dominada por NFS (Network File System) mientras que samba es la opción más habitual en redes que combinan Linux y Windows.

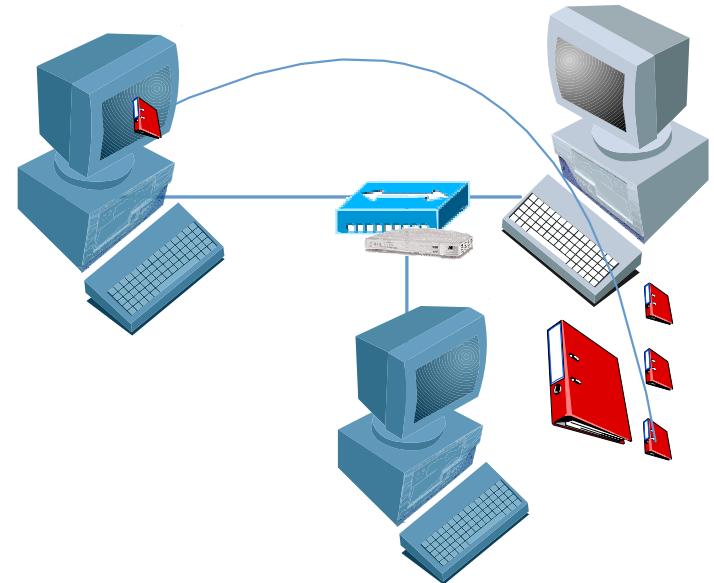


Ilustración 52: Compartir recursos en Linux: Un fichero remoto debe aparecer como perteneciente al árbol de directorios local

Anotaciones

Sistema de archivos en red (NFS).

NFS es un sistema de archivos que permite compartir recursos en la red mediante el protocolo TCP/IP. Es un estándar abierto creado por SunSoft que implementa una arquitectura cliente/servidor para el proceso de compartición de ficheros. La configuración de NFS permite que varios sistemas operativos comparten los archivos en una misma red puesto que define un modelo abstracto de sistemas de ficheros que es interpretado por los distintos sistemas operativos.

El sistema de archivos NFS consta de un servidor, que proporciona los archivos, un cliente que los monta en su sistema de ficheros local y un protocolo de comunicación que permiten al cliente manipular los ficheros en el servidor.

Analogía:

Realmente el cliente no manipula los archivos en el servidor. Es el propio servidor el que actúa y envía los resultados al cliente. Básicamente, la máquina cliente es como una persona que da instrucciones para aparcar un vehículo, mientras que el servidor sería el conductor que ejecuta las órdenes.

El servidor NFS dispone de un sistema que permite indicar desde qué máquinas o dominios se puede acceder a los ficheros compartidos y en qué modo lo van a hacer. Monta de forma virtual una unidad en el host local con los directorios compartidos ocultando la posición del fichero en la red y del servidor.

Sistema de ficheros de Andrew (AFS)

Se trata de un sistema de ficheros distribuidos que presenta de forma compacta todos los recursos compartidos en la red (LAN y WAN) a través de un directorio /afs sobre TCP/IP.

Todos los recursos compartidos en un dominio se presentan en una celda AFS que agrupa a los servidores de recursos presentando un único sistema de ficheros. AFS emplea el sistema de seguridad Kerberos de manera que los password circulan encriptados por la red. La autenticación de usuarios debe ser realizada contra el servidor que mantiene un listado de los usuarios que acceden al servicio.

Mejora a NFS en tanto en cuanto el usuario no debe conocer el servidor en el que se encuentra el archivo compartido, sino que todos se presentan juntos y sólo se debe conocer la ruta de acceso. Soporta con garantías una razón 50:1 de cliente/servidor y ofrece opciones de escalabilidad mejoradas con respecto a NFS.

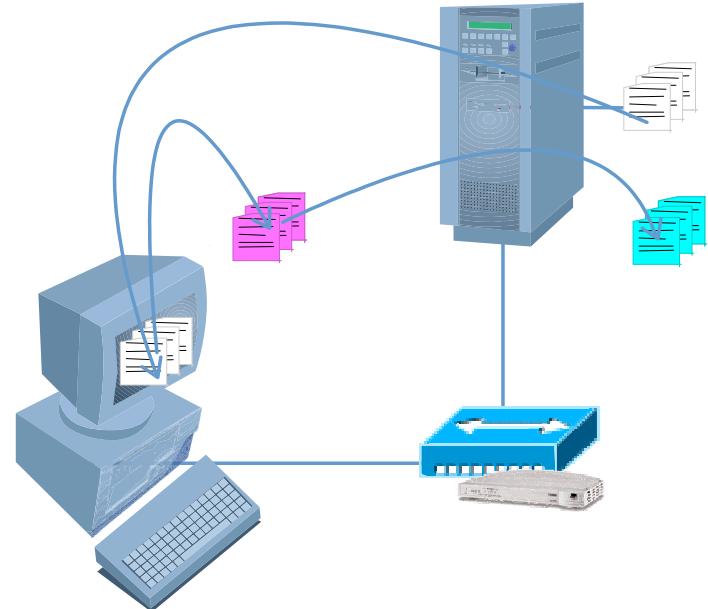


Ilustración 53: NFS: Monta los ficheros remotos en el árbol de directorios local y permite su edición remota

Anotaciones

Samba.

Samba permite la compartición de ficheros e impresoras en redes constituida por múltiples sistemas operativos. Un servidor Samba permite:

- Compartir sistemas de ficheros.
- Compartir impresoras instaladas en cualquier lugar de la red.
- Autenticar clientes en un dominio windows.

Smb.cnf es el fichero que controla los demonios de samba. Está compuesto de secciones y parámetros. Cada sección define un servicio y los parámetros son los atributos con los que se puede acceder a dicho servicio, siendo este un espacio de ficheros o servicios imprimibles.

Difiere de las dos opciones anteriores en que no consiste en un sistema de ficheros, sino una utilidad para compartir recursos. Para configurarse como tal necesita smfbs que sí es un sistema de ficheros que analiza los recursos compartidos por servidores samba y los presenta a los usuarios en una estructura de directorios.

c) Sistema de directorios.

Como ya hemos indicado, las redes Linux no emplean herramientas de administración como el Active Directory de Windows, puesto que su propia estructura de archivos lleva implícito un sistema similar. El administrador de una red Linux dispone de algunas herramientas que permiten una administración en entorno gráfico (Webmin), sin embargo, la mayoría de los administradores prefieren la utilización de líneas de comando puesto que controlan más todo el proceso.

Linux es un sistema operativo multiusuario y de trabajo en red desde sus orígenes, por lo que el sistema de archivos ya lleva incorporadas capacidades. La administración se puede realizar desde un principio en el momento en el que un usuario se identifica para acceder a los recursos. El proceso de autenticación puede ser implementado a través de LDAP contra una base de datos de usuarios (MySQL), de manera que, al iniciar su sesión, se cargue su perfil en cualquier máquina.

Además, en este proceso de inicio, se montan tanto las unidades locales como las unidades de red de forma transparente, el usuario accede a sus recursos que pueden estar en cualquier otra máquina y que se montan en la carpeta home. El sistema de directorios que aparece en la máquina local una vez que se inicia Linux y se identifica el usuario recogerá todos los recursos que el administrador considere que deben ser empleados por ese usuario, en función de los permisos que tenga asignados. Es decir, tras el proceso de identificación se montan los directorios y recursos asociados a ese usuario con independencia del lugar en el que se encuentren.

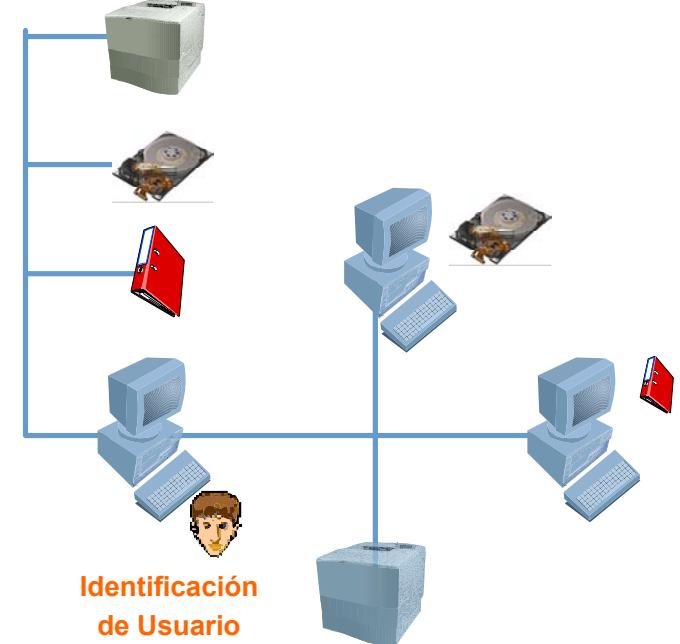


Ilustración 54: Montaje de unidades: En el proceso de inicio se montan todas las unidades compartidas una vez que accede el usuario

Anotaciones

El sistema de directorios permite gestionar los recursos de la red de forma similar a la administración que con Active Directory se hace de los dominios. Las distintas unidades que se montan en la red y que son compartidas pueden moverse de un lugar a otro, las propiedades de un grupo pueden ser modificadas en cualquier momento y la gestión de permisos se hace completamente flexible.

d) Seguridad del Sistema.

Una red debe disponer de unas opciones de seguridad que garanticen la estabilidad del sistema. En muchos casos la estabilidad puede deberse a actuaciones de los usuarios o a la intervención de crackers que acceden a nuestra red.

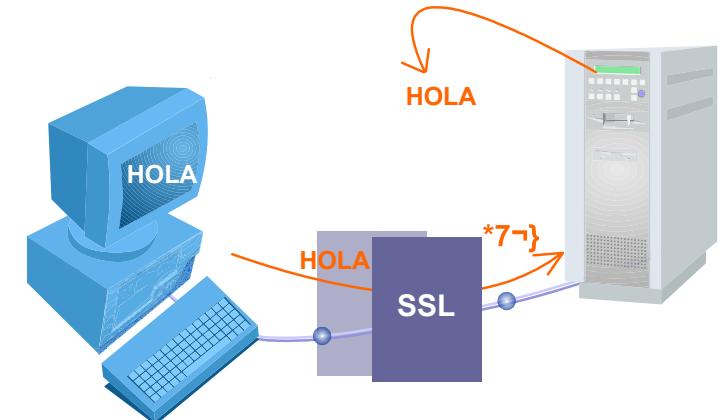
Hasta ahora nos hemos centrado en los aspectos relacionados con los usuarios y las políticas de permisos. El punto débil de estas políticas es la transmisión de claves a través de la red. Ya comentamos que ADF utilizaba el Kerberos para encriptar las claves que se emplean en la compartición de ficheros. Sin embargo, existen otras opciones que deben ser implementadas cuando estamos administrando remotamente nuestra red.

SSL (Secure Server Layer) es un protocolo que permite cifrar las comunicaciones entre cliente y servidor. En el mundo Linux existen varias opciones que, implementando este tipo de protocolo, permiten establecer conexiones seguras entre clientes y servidores, especialmente útiles cuando se está realizando cualquier labor de administración remota.

Algunas de las soluciones de seguridad emplean OpenSSL, OpenSSH o Net_SSLeay. En cualquier caso se trata de proteger las comunicaciones con independencia de la aplicación o protocolo de comunicación que se emplee FTP, web, o ejecutando X-window en un servidor remoto.

Con respecto a los ataques que puedan venir desde el exterior, la opción mejor es la utilización de un cortafuegos que proteja a usuarios y datos de los peligros de Internet. Existen dos tipos de cortafuegos en Linux, de filtrado de paquetes y proxy.

En el primer caso se analizan los datos de la cabecera IP y se establecen unos criterios para su filtrado. El proxy, por otro lado, recibe todos los paquetes, los filtra y los reencamina dentro de la red, pudiendo llegar a analizar todo el paquete, no sólo su cabecera. Como ya veremos en el capítulo 6, su uso puede ser conjunto, pero la opción a la hora de elegir uno u otro es personal, y va a depender, sobre todo, de la experiencia previa que se disponga a la hora de manejar uno u otro tipo.



Anotaciones

4.7. Protocolos de comunicación en redes con Linux.

Siendo el resultado del esfuerzo concentrado de programadores de todo el mundo, Linux no habría sido posible sin la red global. Así que no sorprende que ya en los primeros pasos del desarrollo, varias personas comenzaron a trabajar en dotarlo de capacidades de red.

Linux dispone de los dos principales protocolos de red para sistemas UNIX: TCP/IP y UUCP.

a) UUCP.

UUCP (UNIX-to-UNIX Copy) es un viejo mecanismo usado para transferir ficheros, correo electrónico y noticias entre máquinas UNIX. Clásicamente las máquinas UUCP conectan entre ellas mediante líneas telefónicas y módem, pero UUCP es capaz de funcionar también sobre una red TCP/IP. Si no tiene acceso a una red TCP/IP o a un servidor SLIP, puede configurar su sistema para enviar y recibir ficheros y correo electrónico usando UUCP. Su principal aplicación es todavía en redes de área metropolitana (MAN) basadas en enlaces telefónicos.

Una de las principales desventajas de las redes UUCP es su bajo ancho de banda. Por un lado, el equipo telefónico establece un límite rígido en la tasa máxima de transferencia. Por otro lado, los enlaces UUCP raramente son conexiones permanentes; en su lugar, los nodos se llaman entre sí a intervalos regulares. Es por ello, que la mayoría del tiempo que le lleva a un mensaje viajar por una red UUCP permanece atrapado en el disco de algún nodo, esperando al establecimiento de la próxima conexión.

A pesar de estas limitaciones, aun hay muchas redes UUCP funcionando en todo el mundo, utilizado principalmente por aficionados, ya que ofrecen acceso de red a usuarios privados a precios razonables. La razón fundamental de la popularidad del UUCP es que es baratísimo comparado con tener el ordenador conectado al Gran Cable de Internet.

Para hacer de su ordenador un nodo UUCP, todo lo que necesita es un módem, software UUCP, y otro nodo UUCP que desee suministrarle correo y noticias.

b) TCP/IP.

Aunque UUCP puede resultar una elección razonable para enlaces de red mediante llamada de bajo coste, hay muchas situaciones en las que su técnica de almacenamiento y reenvío se muestra demasiado inflexible, por ejemplo en Redes de Área Local (LANs).

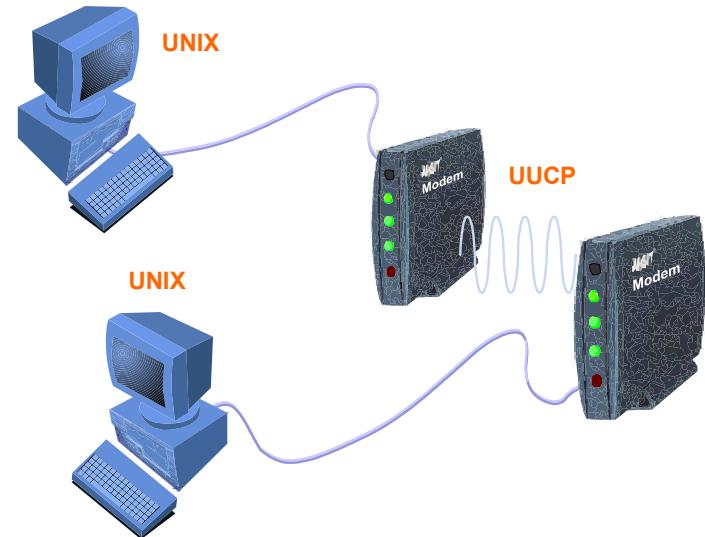


Ilustración 56: UUCP: Es un protocolo para comunicar máquinas UNIX a través de redes WAN

Anotaciones

TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos de red que permite a sistemas de todo el mundo comunicarse en Internet. Con Linux, TCP/IP y una conexión a la red, puede comunicarse con usuarios y máquinas por toda Internet mediante correo electrónico, noticias (USENET news), transferencias de ficheros con FTP y mucho más. Actualmente hay muchos sistemas Linux conectados a Internet.

No todo el mundo tiene una conexión Ethernet en casa, así que Linux también proporciona SLIP (Serial Line Internet Protocol), el cual permite conectarse a Internet a través de un módem. Para poder usar SLIP, necesitará tener acceso a un servidor de SLIP, una máquina conectada a la red que permite acceso de entrada por teléfono. Muchas empresas y universidades tienen servidores SLIP disponibles. De hecho, si su sistema Linux dispone de conexión Ethernet y de módem, puede configurarlo como servidor de SLIP para otros usuarios.

Fue en el otoño de 1992 cuando se comenzó a desarrollar el soporte de TCP/IP, cuando Ross Biro y otros crearon lo que ahora se conoce como Net-1. Actualmente ya existe Net-3, que ofrece controladores de dispositivo para una amplia variedad de tarjetas Ethernet, así como SLIP (para enviar tráfico de red sobre líneas serie), y PLIP (para líneas paralelo).

Con Net-3, Linux tiene una implementación de TCP/IP que se comporta muy bien en entornos de red de área local, mostrándose superior a algunos de los Unix comerciales para PCs.

5. Otros sistemas operativos.

5.1. Microsoft LAN Manager.

Se trata de un sistema operativo diseñado para redes cliente/servidor. Trabaja bajo OS/2 en el servidor de archivos aunque las estaciones clientes admiten múltiples sistemas. Estas redes deben disponer de un Servidor y en todas las estaciones clientes del redirector, que se encarga de interceptar y redirigir las peticiones de los clientes. Al proporcionar el servidor la mayoría de las aplicaciones, las estaciones clientes pueden ser equipos de baja prestaciones.

La administración de esta red es sencilla y permite la agrupación de varios servidores en un mismo dominio, tratándolos como si fueran una única máquina; igualmente, dispone de un sistema sencillo de copias de seguridad entre servidores o se permite la administración remota de todas las estaciones que dispongan de OS/2.

Anotaciones

La administración de usuarios permite configurar accesos restringidos a directorios, desde unas determinadas máquinas, en un intervalo horario, con una serie de privilegios, etc.

5.2. IBM LAN Server.

Sistema operativo bajo OS/2 derivado de Microsoft LAN Manager. Crea redes estructuradas en dominios controlados por un equipo servidor al que se conectan cada uno de los clientes que deben disponer de una aplicación OS/2 LAN Requester o DOS LAN Requester para poder acceder a la red. Las redes dependientes de este sistema operativo requieren, necesariamente, de la creación de un dominio.

Los recursos compartidos disponen de diferentes niveles de acceso en función del usuario registrado que realice la petición. Además del administrador existen usuarios operadores que pueden administrar cuentas y recursos dentro de un dominio.

5.3. Redes Apple.

System 9, el sistema operativo de Apple permite configurar cualquier PC como servidor o cliente en una estación de red aunque con un número limitado de usuarios. Los distintos servicios y aplicaciones de la red deben ser activados en cada una de las máquinas para que estén operativos.

Appel Talk es la denominación de las redes de Apple. Las redes de este tipo de gran volumen necesitan de un sistema operativo servidor que las gestione. Este servidor se denomina Apple Share que en sus últimas versiones incluye funciones de administración vía web y seguridad funcionando sobre redes TCP/IP o Apple Talk.

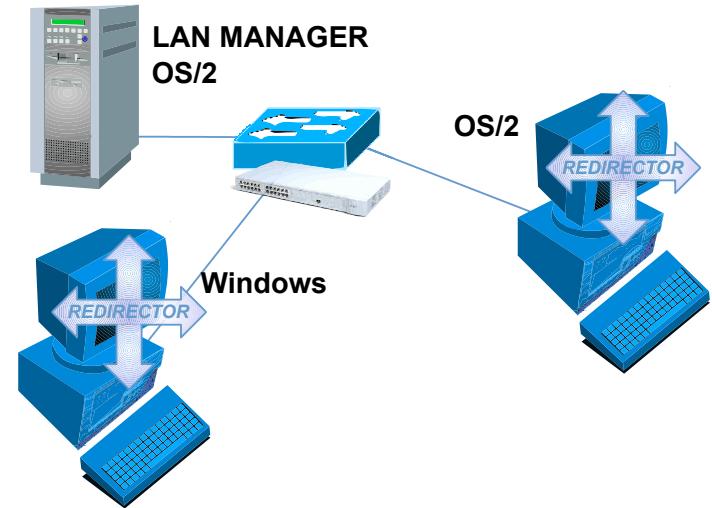


Ilustración 57: El redirector se encarga de capturar las comunicaciones en el host local para dirigirlas hacia la red.

Anotaciones

Ilustraciones

Ilustración 1: El S.O. es el software que ejerce de intermediario entre el resto de las aplicaciones y el hardware	5
Ilustración 2: Sistema operativo de estructura jerárquica en anillos concéntricos.	6
Ilustración 3: Un sistema operativo multitarea puede ejecutar varias tareas a la vez dedicando un tiempo a cada una de ellas en función de su prioridad.	7
Ilustración 4: Para que un equipo se pueda conectar a una red requiere de la instalación de un S.O. que admita una de las opciones de cliente o servidor de red.	8
Ilustración 5: En un S.O. Cliente-Servidor puro, una estación de trabajo no puede "ver" al resto, sólo puede acceder al servidor	9
Ilustración 6: En una red de igual a igual con servidor, existe un equipo que se encarga de gestionar el acceso a la red y sus recursos, aunque no es, necesariamente, el único equipo que proporciona servicios a la red.	10
Ilustración 7: Un servidor gestiona el acceso a la red por parte de los usuarios	11
Ilustración 8: Actualmente existe una alta interoperabilidad entre sistemas operativos para el trabajo en red.	12
Ilustración 9: El redirector es la aplicación que hace transparente el uso de la red, gestionando y redirigiendo las peticiones de servicio.	13
Ilustración 10: Servicio de Directorio: Es una base de datos centralizada en la que se recogen todos los recursos disponibles en una red	14
Ilustración 11: Sistema de archivos	15
Ilustración 12: En una red Novell los únicos equipos que pueden compartir archivos son los servidores	16
Ilustración 13: Login y acceso a un directorio del servidor: cada usuario dispone de un subdirectorio privado al que accede una vez que se ha identificado	17
Ilustración 14: Replicación: una partición de NDS puede estar replicada en varios servidores.	18
Ilustración 15: Niveles de seguridad: petición de acceso a un servidor y consulta de este a NDS para dar el permiso	19
Ilustración 16: Relación entre el modelo OSI y la pila de protocolos IPX/SPX	20
Ilustración 17: Formato de datagrama IPX	21
Ilustración 18: En las redes Novell se requieren tres direcciones distintas para el envío de un datagrama.	22
Ilustración 19: Formato de paquete de datos SPX	23
Ilustración 20: Mensaje SAP: cada cierto tiempo un servidor indica a través de un mensaje SAP los servicios que ofrece a la red	24

Anotaciones

Capítulo 5

Ilustración 21: Función de RIP: RIP permite enviar las tablas de routing de un dispositivo a otro	25
Ilustración 22: Las redes Windows pueden funcionar con independencia de un equipo con software servidor	26
Ilustración 23: NTFS permite asignar distinto espacio de disco a cada usuario	27
Ilustración 24: Un mismo archivo se encuentra dividido en distintos “Clusters” que deben ser localizados	28
Ilustración 25: Servicio de Windows: puede proporcionar servicio de Correo, de archivos, de Web, de impresión, ...	29
Ilustración 26: Control de acceso a los recursos en redes de “igual a igual”: cada usuario controla el acceso a sus carpetas, administra sus objetos	31
Ilustración 27: Un servidor NT controla la autenticación de usuarios para el acceso a un dominio	32
Ilustración 28: Control de acceso: En un grupo cada ordenador dispone de una base de datos de seguridad local en la que se identifican todos los usuarios, en un dominio la base se encuentra centralizada	33
Ilustración 29: Carpeta pública y privada: una carpeta pública es aquella que es accesible al resto de los usuarios	34
Ilustración 30: Para que un usuario pueda emplear una impresora la debe agregar a su equipo	35
Ilustración 31: Kerberos: Funcionamiento del protocolo de autenticación de red	36
Ilustración 32: Arquitectura de Windows 2000	37
Ilustración 33: Active Directory es una base de datos que almacena de forma jerárquica los recursos de la red y permite su administración.	38
Ilustración 34: Diagrama de espacios de nombres de dominio	39
Ilustración 35: Dominio: Es una agrupación lógica de ordenadores que tienen una base de datos centralizada	40
Ilustración 36: Sistema de nombres de dominio DNS: este protocolo, permite a los ordenadores clientes, que tienen direcciones IP asignadas dinámicamente , poder registrarse en un servidor DNS y actualizar la base de datos DNS	41
Ilustración 37: Windows 3.1: necesita de MS-DOS para poder operar con el hardware	45
Ilustración 38: Windows 95: es un Sistema Operativo de 32 bits que mejora la capacidad de proceso de los Sistemas Operativos de 16 bits	46
Ilustración 39: Monitor en red: Muestra el estado de los recursos que el ordenador tiene compartidos	53
Ilustración 40: Red Windows: Una red Windows configurada como grupo de trabajo la configuración de cada PC condiciona el funcionamiento de la red	54
Ilustración 41: El modo sesión Net BIOS transmite los mensajes de forma ordenada llegando al host receptor organizados	55

Anotaciones

Capítulo 5: Sistemas operativos de red

Ilustración 42: CHACHÉ NETBIOS: Almacena los nombres en una tabla dinámica	56
Ilustración 43: Tabla LMHOST: Antes de realizar BROADCAST el host analiza su tabla LMHOST, si no encuentra el nombre, lo solicita a la red	57
Ilustración 44: Linux: Es un sistema Operativo multiusuario	60
Ilustración 45: Consolas virtuales múltiples Linux admite varias consolas virtuales	61
Ilustración 46: Árbol directorio de Linux: Es una estructura jerárquica	62
Ilustración 47: Carpeta/home: Almacena los archivos de cada usuario	63
Ilustración 48: Montaje de dispositivos: Cualquier dispositivo de un PC debe ser montado como un archivo para poder ser utilizado	64
Ilustración 49: Shell: Es un interprete de órdenes para que el usuario interactúe con el sistema	65
Ilustración 50: Gestor de ventana: Permite interactuar en forma gráfica	66
Ilustración 51: Sistema de Permisos en Linux: Un archivo tiene asignados permisos de lectura, escritura y acceso a su propietario, grupo al que pertenece y todos los usuarios	69
Ilustración 52: Compartir recursos en Linux: Un fichero remoto debe aparecer como perteneciente al árbol de directorios local	70
Ilustración 53: NFS: Monta los ficheros remotos en el árbol de directorios local y permite su edición remota	71
Ilustración 54: Montaje de unidades: En el proceso de inicio se montan todas las unidades compartidas una vez que accede el usuario	72
Ilustración 55: SSL: Permite datos de comunicaciones seguras en una red Linux encriptando los datos que circulan	73
Ilustración 56: UUCP: Es un protocolo para comunicar máquinas UNIX a través de redes WAN	74
Ilustración 57: El redirector se encarga de capturar las comunicaciones en el host local para dirigirlas hacia la red.	76

Anotaciones