TEMA

65

Análisis comparativo entre un sistema operativo multiusuario y un sistema en red.

elaborado por
EL EQUIPO DE PROFESORES
DEL CENTRO DOCUMENTACIÓN

1. INTRODUCCIÓN

El análisis comparativo se basa en como gestiona diversos recursos uno y otro sistema.

En ambos sistemas la administración de sistemas supone un conocimiento muy importante de lo que significa y las características del mismo.

Las redes locales aparecen como evolución natural de conexión entre el gran número de ordenadores personales. Una vez que el uso del ordenador personal se extiende y en cualquier empresa se dispone de un número considerable de estos, una la red local permite conectarlos entre sí, y compartir de esta forma recursos, aumentar el nivel de comunicación, facilitar la gestión, etc.

Siendo de esta forma es obvio que muchas de las características de los ordenadores personales se hayan trasladado a la red local.

Si tenemos en cuenta que un gran número de ordenadores personales utilizan el sistema operativo DOS, es fácil comprender porqué en una red local podemos utilizar muchos de los comandos del DOS.

Efectivamente, una de las características más importantes y atractivas de las red local es que el usuario no necesita grandes esfuerzos para comprender el nuevo entorno. Para este a partir de ahora "verá" una nueva unidad (unidad lógica) en su ordenador (F:, E:, G:, I: ;...) que significa la unidad de red.

La mayor parte de los comandos que utilizaba en su sistema monousuario, los puede seguir usando ahora sin problemas. En todo sistema informático de nueva implantación la repercusión que tendrá sobre personal que va a utilizarlo es uno de los aspectos más estudiados.

El coste de formación al nuevo sistema, y sobre todo la predisposición de los empleados por cambiar "lo que se conoce y domina", influye enormemente a la hora de adquirir nuevos sistemas.

Las redes locales en este aspecto tienen ganada la partida a sistemas multiusuarios, tipo UNIX.

Un sistema multiusuario tiene pocas similitudes con un sistema monousuario. El entorno de trabajo varía notablemente.

Sin embargo algunos de estos sistemas, como es el caso del UNIX, es anterior a sistemas monousuario, como es el caso de DOS, y este heredó algunas características de aquel.

La organización de archivos en directorios y subdirectorios es un ejemplo muy claro de esta herencia.

En lo que respecta al estudio entre ambos sistemas, Red y Multiusuario, conviene aclarar que un sistema en red es también un sistema multiusuario.

Si analizamos los puntos más importantes de ambos veremos diferencias; pero también muchas coincidencias.

Por último, para este estudio se ha utilizado como referencia de sistema en red, el sistema operativo NetWare de Novell. El UNIX sirve como modelo de sistema multiusuario.

2. USUARIOS Y GRUPOS

En este apartado la similitud de funcionamiento entre un sistema en Red y un sistema multiusuario es importante. En ambos existe un "superusuario" que tiene todos los derechos o privilegios, usuarios normales y usuarios especiales a los que el "superusuario" les asigna derechos adicionales.

2.1. TIPOS DE USUARIOS

2.1.1. Sistemas en Red

Una red tiene usuarios con distintos tipos de acceso y control.

Básicamente se pueden dividir en tres:

- **Supervisor**

Posee derecho ilimitados sobre todos los recursos de la red (Usuarios normales, archivos, comunicaciones, etc.).

- **Operador**

Un operador de red es un usuario estable de la red al que se le han asignado derechos adicionales.

- **Usuarios normales**

Usuarios que utilizan la red pero que no tiene opción de gestionar los recursos de la misma.

El supervisor o administrador tiene acceso completo a los archivos del sistema, y controla el sistema de seguridad. El usuario supervisor puede establecer niveles de seguridad, restricciones sobre estaciones de trabajo, restricciones de usuario y facturación de uso de recursos, entre otras posibilidades.

Una de la responsabilidades es la de incorporar nuevos usuarios y eliminar los que ya no deban tener acceso.

2.1.2. Sistema Multiusuario

En un sistema multiusuario, ejemplo UNIX, encontramos los siguientes tipos de usuarios:

a) Superusuario, supervisor, o root:

Es el administrador del sistema. Tiene todos los privilegios.

b) Usuarios normales:

Son los usuarios normales del sistema. Se pueden asignar en grupos, que pueden tener una serie de propiedades comunes.

c) Usuarios especiales:

Asignados a tareas específicas por el sistema, generalmente de información o manejo de aplicaciones ya instaladas de uso común a usuarios externos o internos.

Desde el punto de vista del usuario, se ven los siguientes usuarios:

El propio usuario	u
El conjunto de usuarios del mismo grupo	g
El resto de usuarios	o

2.2. GESTIÓN DE USUARIOS

2.2.1. Sistemas en Red

La función de crear nuevos usuarios en la red es exclusiva del usuario supervisor.

Cada vez que se crea un usuario en la red debemos darle unos derechos y restricciones. Pero además podemos asignarle propiedades específicas.

Entre ellas podemos citar:

- Secuencia de conexión

Una secuencia de conexión son los pasos (órdenes) que un usuario puede ejecutar antes de entrar en red. Por ejemplo podemos asignarle cada vez que conecte con la red que se visualiza en todo momento el directorio donde se encuentra, asignarle unidades de red, mensajes de aviso, correo electrónico, etc.

- Directorio personal

Podemos asignarle un directorio para que trabaje con todos los derechos sobre él (creación, modificación, borrado, etc.).

- Clave de acceso

Cada vez que el usuario conecte con el sistema debe identificarse con su nombre e introducir correctamente su clave de acceso. Esta podemos obligarle a que la cambie cuando pase un cierto número de días, e incluso a que no la cambie por las 8 ultimas.

- Nombre completo

A los usuarios se les asigna una identificación de acceso, por ejemplo "PEPECONTB"; pero además dentro de la red se le puede identificar con un nombre más largo. Ejemplo "Pepe el del sexto".

- Asignación de grupos

Podremos asignar al usuario uno o varios grupos para facilitar la gestión.

- Restricciones sobre estaciones

En un sistema en red podemos obligar a que un determinado usuario siempre conecte desde un determinado terminal (nodo).

- Restricciones temporales

A los usuarios se les especifica en qué momentos puede usar o no el sistema. Incluso es habitual restringir el acceso a todos los usuarios a la vez durante un intervalo de tiempo. Ejemplo: los sábados de 16 a 18 para gestión especial del sistema.

Lo visto hasta aquí respecto a los usuarios es válido de forma general para los grupos en una red local. La diferencia, ya vista, es que cuando lo aplicamos a un grupo afecta a varios usuarios a la vez (a todos aquellos que pertenecen al grupo).

2.2.2. Sistema Multiusuario

El comando **useradd** o **adduser**, según versiones, añade un nuevo usuario al sistema, así como modifica algunos de sus parámetros: grupo al que pertenece, directorio de trabajo, password, etc.

Mediante **userdel** se puede suprimir un usuario del sistema, con la opción **-r**, que permite borrar todo su directorio de home (personal).

Para gestionar los grupos en UNIX, se utiliza básicamente los comandos **groupadd** y **groupdel**. Con **groupadd** creamos un nuevo grupo al sistema, con **groupdel** podemos suprimir un grupo.

Las características que definen a todo usuario son:

Nombre:	Nombre para el sistema.
Clave:	Clave personal de acceso al sistema.
UID:	Número de identificación del usuario.
GID:	Número de identificación del grupo.
Directorio:	Directorio inicial al entrar al sistema.

Nombre completo.
Login shell.

3. ESTUDIO DE LOS DERECHOS

3.1. SISTEMAS EN RED

Los usuarios de la red necesitan derechos de acceso para acceder a los recursos de la red y para trabajar con los archivos del sistema de archivos. Los derechos determinan exactamente la forma en que el usuario podrá acceder a los directorios y archivos del sistema de archivos.

El único que tiene posibilidad de asignar o cancelar derechos es el usuario supervisor.

Algunos de estos derechos pueden ser:

- Supervisor. Supone todos los derechos sobre el directorio, sus archivos y sus subdirectorios. A este derecho también se le denomina completo.
- Lectura. Permite ejecutar programas en el directorio y abrir los archivos que contiene, así como leerlos.
- Escritura. Permite abrir y cambiar el contenido de los archivos que existan en el directorio.
- Creación. Permite crear nuevos archivos y subdirectorios en el directorio.
- Borrado. Permite borrar el directorio, sus archivos y sus subdirectorios.
-Modificación. Permite modificar los atributos y nombres del directorio, sus archivos y sus subdirectorios, pero no cambiar su contenido.
- Búsqueda. Con este derecho se puede ver el directorio y sus archivos con las órdenes DIR y NDIR.

3.1.1. La Orden FLAG

En un sistema los atributos de los archivos van a determinar qué usuarios y en qué modo pueden acceder a los mismos.

Por ello debe disponer de órdenes o utilidades encaminadas a la gestión de atributos. En el caso de NetWare, la orden es FLAG.

En su forma más simple, FLAG muestra los atributos de todos los directorios.

Para asignar un atributo a un directorio se utiliza la sintaxis:

FLAG vía_de_acceso + atributo

Para cancelar un atributo se utiliza la sintaxis es:

FLAG vía_de_acceso - atributo

En ambos casos atributo puede ser uno de los siguientes: N (Normal), Hi (oculto), Sy (Sistema).

En el caso de archivos la orden se utiliza de igual forma. Respecto a los atributos se incluyen entre otros: Ro (sólo lectura), Sh (Compartido), X (sólo ejecución).

En un sistema en red un archivo que no tiene activado el atributo de compartido (Sh), sólo puede ser utilizado por un usuario a la vez. Mientras dicho usuario está haciendo uso del archivo nadie puede utilizarlo.

3.1.2. Orden RIGHTS

La orden RIGHTS se utiliza desde el indicador de órdenes para ver o modificar los derechos que los usuarios o grupos poseen sobre archivos y directorios.

La orden RIGHTS utilizada sin parámetros muestra los derechos que se poseen sobre un directorio.

Para asignar derechos con la orden RIGHTS se utiliza el siguiente formato:

RIGHTS vía_de_acceso + lista_de_derechos /NAME=usuario/s

Para cancelar derechos se utiliza la sintaxis:

RIGHTS vía_de_acceso - lista_de_derechos /NAME=usuario/s

Los derechos que se pueden asignar o cancelar puede ser cualquiera de los siguientes: ALL (todos), A (control de acceso), C (Creación), E (Borrado), F (Búsqueda de archivos), M (Modificación), R (Lectura), S (supervisor), W (Escritura).

Por ejemplo para darle a Fran todos los derechos sobre el directorio APLIC se escribe la orden:

RIGHTS APLIC ALL /NAME=FRAN

3.2. SISTEMAS MULTIUSUARIO

Uno de los aspectos más importantes de un sistema operativo multiusuario es la gestión de permisos de acceso o restricciones sobre la información.

Dado que UNIX es un sistema multiusuario, debe contar con algún mecanismo para proteger la información (ficheros y directorios) de un usuario particular, del acceso no autorizado de otros usuarios.

De esta manera si un usuario crea ficheros y directorios en su directorio home, el usuario es el dueño de esos ficheros y directorios; y por lo tanto tiene acceso a ellos.

De todas maneras UNIX permite que los ficheros puedan ser compartidos entre usuarios, ya sean del mismo grupo o no, pero siempre a decisión del dueño. Por defecto cuando un usuario crea un fichero, éste podrá ser consultado por otros usuarios, pero nunca podrá ser modificado o borrado, ni ejecutado. Cuando se crea un directorio, por defecto, se permite a otros usuarios entrar en el para consultar y ejecutar ficheros.

Como se ha explicado cada fichero pertenece a un usuario particular, pero también pertenece a un grupo en particular, que es el grupo de usuarios que pertenecen al mismo grupo que el dueño. Cada usuario forma parte por lo menos de un grupo, esta inclusión se realiza cuando se crea la cuenta del usuario. Sin embargo, el root puede hacer que un usuario esté en más de un grupo, pero un fichero solo puede pertenecer a un grupo.

Por defecto pertenecerá al grupo principal o inicial del usuario. Si el usuario pertenece a más de un grupo podrá cambiar el grupo del fichero mediante el comando **chgrp**.

Los grupos se definen generalmente por los tipos de usuarios que acceden al sistema. Existen también una serie de grupos definidos por el sistema (bin, admin) que son propios del sistema para controlar el acceso a ciertos recursos.

El esquema que se emplea consiste en dividir el universo de los usuarios en tres categorías:

- La clase **u**: formada por el usuario.
- La clase **g:** formada por los usuarios que pertenecen al mismo grupo que el dueño de los ficheros.
- La clase **o**: compuesta por el resto de los usuarios.

Los permisos por su parte se dividen en tres categorías, lectura, escritura y ejecución. Así a cada tipo de usuario (u, g, o) le corresponderá una triada donde se refleje sus privilegios de lectura, escritura y ejecución con respecto a un fichero o un directorio particular.

- El permiso de lectura **r**:

Permite a un usuario consultar el contenido de un fichero, o en el caso de los directorios listar el contenido del mismo.

- El permiso de escritura **w**:

Permite a un usuario modificar o borrar un fichero, en el caso de los directorios permiten crear o borrar ficheros.

- El permiso de ejecución **x**:

Permite al usuario ejecutar un fichero ejecutable o un script, en el caso de los directorios, tener permiso de ejecución permite entrar en el directorio, es decir hacer cd al directorio en cuestión.

Para ver los permisos de un fichero se tiene que utilizar la orden **ls -l**, esta orden es de las más utilizadas en UNIX, por este motivo existe un alias para este comando en la mayoría de los sistemas UNIX, este alias es ll.

La salida que da el comando ls -l es la siguiente:

-rw-r--r-- 1 fran users 708 Mar 10 19:00 mifichero

El primer campo representa a los permisos, el tercer campo es el dueño, siendo el cuarto campo el correspondiente al grupo, y el último campo es el nombre del fichero.

La cadena de permisos es **-rw-r--r--** que representa los permisos del usuario, del grupo y del resto de los usuarios, por este orden.

El primer carácter de la cadena de permisos es un - y representa el tipo de fichero. El que haya un - significa que es un fichero normal. Otros símbolos que pueden aparecer son:

s: Si es un socket.
l: Si es un enlace simbólico.
d: Si es un directorio.
c: Si es un dispositivo de caracteres.
b: Si es un dispositivo de bloque.

A continuación se tienen tres triadas, la primera representa los permisos del usuario, la segunda los permisos del grupo, y la tercera los permisos del resto de los usuarios.

Dentro de cada triada el orden es lectura, que se representa por **r**, escritura, que se representa por **w**, y ejecución, que se representa por **x**. Cuando en la triada aparece la letra que representa al permiso, significa que ese permiso está activo, si por el contrario aparece un signo - significa que el usuario no cuenta con ese permiso.

Por lo explicado en el párrafo anterior, en el ejemplo, el usuario fran, que es el dueño del fichero, tiene permiso de lectura y escritura, todos los usuarios del grupo users, grupo al que pertenece fran, tienen permiso de lectura, y por último el resto de los usuarios tienen permiso de lectura sobre el fichero mifichero.

Un aspecto importante, y que se tiene que tener en cuenta, es que los permisos de un fichero también dependen de los permisos del directorio en el que está alojado. Por ejemplo si un fichero tiene el siguiente conjunto de permisos **-rwxrwxrwx**, el resto de los usuarios no podrán hacer uso de ellos a menos que ellos tengan permiso para leer, escribir o ejecutar ficheros en el directorio en el que se encuentra dicho fichero. Así si el directorio donde se encuentra el fichero tiene los permisos **-rwx------**, aunque el fichero tenga todos sus permisos activos, ningún usuario a parte del dueño podrá acceder a él. Por defecto, los ficheros de un usuario tienen la siguiente cadena de permisos **-rw-r--r--**, mientras que los directorios tienen la siguiente cadena de permisos **-rwxr-xr-x**.

3.2.1. La orden chmod

Para cambiar la cadena de permisos se utiliza el comando **chmod**. Sólo el dueño puede cambiar los permisos de un fichero. Este comando tiene dos sintaxis diferentes, una basada en cadenas mnemotécnicas, que es más intuitiva, y otra basada en combinaciones en base octal, que es más potente.

La sintaxis basada en cadenas mnemotécnicas es:

chmod [a, u, g, o] +¦- [r, w, x] <nombre de ficheros>

Donde:

a: Significa todos los usuarios.
u: Significa el dueño.
g: Significa el grupo.
o: Significa el resto de los usuarios.
+: Significa activar un permiso.
-: Significa desactivar un permiso.
r: Significa permiso de lectura.
w: Significa permiso de escritura.
x: Significa permiso de ejecución.

Ejemplos:

chmod a +r mifichero
Da a todos los usuarios permiso de lectura sobre el fichero **mifichero**.

chmod +r mifichero
Lo mismo que el anterior. Cuando no se indica a quien, se asume todos (**a**) por defecto.

chmod og-x mifichero
Se desactiva el permiso de ejecución para el grupo y para el resto de los usuarios.

chmod u+rwx mifichero
Se activan todos los permisos para el usuario.

La segunda sintaxis, aunque algo más compleja, permite cambiar de una vez todos los permisos de un fichero, se trata por separado cada grupo de usuarios, se asocian tres bits para cada uno de ellos. Con tres bits se pueden tener ocho combinaciones, desde 000 a 111, donde un 0 significará que el permiso no está activo, y un 1 significará que el permiso está activo. De esta manera se puede representar los permisos de cada grupo de usuarios por un solo dígito octal.

Ejemplo:

Suponer que para el fichero **mifichero** se quieren establecer los siguientes permisos: que todos puedan leerlo, pero que sólo el usuario pueda modificarlo y ejecutarlo.

La estructura de permisos será **u**(rwx), **g**(r), **o**(r). Es decir, **-rwxr--r--**, o lo que es lo mismo 111 100 100, que en octal se representaría por 744. Luego el comando sería:

chmod 744 mifichero

4. GESTIÓN DE ARCHIVOS Y DIRECTORIOS

4.1. SISTEMAS EN RED

Para un sistema en red la estructura de ficheros y directorios tiene las mismas características que el DOS. Debido a la evolución de la Red a partir del mundo de los ordenadores personales han heredado de estos todas sus características.

Por lo tanto todo lo aplicado al sistema DOS se puede aplicar a sistemas en Red; excepto algunos comandos puntuales.

De todas formas los sistemas en Red, aunque hacen uso de los comandos propios del DOS, también disponen de sus propios comandos e incluso utilidades para gestionar archivos y directorios.

Un ejemplo de ello es la utilidad FILER de Netware. FILER es una herramienta para gestión de directorios y archivos, diseñada para responsables y usuarios normales.

Los responsables pueden usar FILER para asignar derechos sobre directorios y archivos a los usuarios, para gestionar archivos y para visualizar información sobre volúmenes. Los usuarios normales también pueden usar esta utilidad, pero las funciones que puedan ejecutar dependen de sus derechos.

En una red local las utilidades de gestion de archivos y directorios están encaminadas a la facilitar el trabajo diario con estos.

Básicamente una utilidad para gestionar archivos y directorios permite realizar las siguientes tareas:

- Ver una lista de los directorios de un volumen.
- Ver una lista de los subdirectorios y archivos incluidos en directorios.
- Crear nuevos directorios.
- Copiar y desplazar directorios y archivos.
- Ver los nombres de las listas de acceso de directorios y archivos.
- Modificar los atributos de directorios y archivos.
- Recuperar archivos borrados.
- Suprimir definitivamente los archivos borrados.

4.2. SISTEMA MULTIUSUARIO

En un sistema multiusuario, como es el caso de UNIX, la gestión de archivos y directorios, aunque puede tener grandes similitudes con el DOS (éste es resultado de aquél), nos encontramos con grandes diferencias: tipos de archivos, comandos, las utilidades de que dispone, etc.

El pilar básico de UNIX es el sistema de archivos jerárquico o en árbol. En esto si es igual a un sistema en RED.

Sin embargo UNIX no dispone de reglas estrictas para poner nombre a los archivos. Todos los caracteres son permitidos excepto el slash (/).

Otra gran diferencia es que las mayúsculas y las minúsculas son tomados como signos distintos. En un sistema en Red sigue las normas del DOS.

En UNIX no hay extensiones como en Red. No hay nada que indique el tipo de archivo.

Para UNIX el atributo de oculto es un punto al comienzo del archivo. Otra diferencia importante.

Por lo que respecta a los directorio y subdirectorios las diferencias son mínimas:

- Todo archivo se encuentra (pertenece) dentro de un directorio.
- Un directorio es una parte lógica del disco que agrupa un numero determinado de ficheros.
- Dentro de un directorio puede haber ficheros o más directorios. En este caso se denominan sub-directorios. Cada subdirectorio puede tener a su vez más subdirectorios.

- El directorio actual es donde se encuentra el usuario en cada momento. Se representa por el carácter . (un punto).
- El directorio padre es el anterior al actual. Se representa por .. (dos puntos seguidos).

Sin embargo par UNIX el directorio raíz se representa por (/). Para la Red con el carácter (\).

Algunos de k¡los comandos propios de UNIX son:

cd - Cambiar de directorio
mkdir - Crear un directorio
rmdir - Borrar un directorio
pwd - Informa del path absoluto del directorio actual partiendo del directorio raíz
ls - Lista el contenido de un directorio
cat - Dirige el contenido de un fichero a la salida estándar
more - Muestra el contenido de un fichero por pantalla, pero haciendo pausa cada vez que se llena la pantalla de información
cp - Copiar ficheros
mv - Mover ficheros
rm - Borrar ficheros

5. GESTIÓN DE IMPRESIÓN

Tanto en un sistema en una Red como en un sistema multiusuario la gestión de impresión es muy similar.

En LAN podemos imprimir en impresoras locales, conectadas en una estación de trabajo, o en una impresora de la red, conectada al servidor.

Las herramientas y programas que se utilizan para configurar las utilidades de impresión de un S.O. de red puede ser muy variado.

Las facilidades de gestión de impresión van encaminadas a:

- Configurar y controlar los servidores de impresión, colas de impresión e impresoras.

- Crear servidores de impresión en las estaciones de trabajo, para ser compartidos con otros usuarios.
- Hacer cambios rápidos sobre la definición de los servicios de impresión.
- Facilitar a los responsables y usuarios de la red las configuraciones de impresión estándar, las cabeceras, papel continuo, etc.
- Utilidades para definir impresoras y códigos de control especiales. Se utiliza fundamentalmente cuando las aplicaciones que se usan en la red no son especiales para redes.
- Permitir a las estaciones de trabajo imprimir archivos de texto ASCII en las impresora de la red.

En un sistema multiusuario como UNIX se incluyen una colección de programas, denominados el sistema lp, para imprimir archivos y documentos.

El sistema lp es en sí mismo grande y complejo, pero afortunadamente su complejidad está oculta a los usuarios. De echo las tres órdenes básicas, **lp**, **lpstat** y **cancel**, es todo lo que se necesita saber para usar este sistema.

La orden básica para imprimir un archivo es lp (line printer). Ejemplo. Para imprimir el archivo mifichero:

lp mifichero

La orden lpstat nos muestra información del estado de la impresora: trabajos que hay para imprimirse, la colas de impresión, etc.

La orden cancel se utiliza para eliminar o detener trabajos de impresión.

En algunos sistemas la utilidad **lpadmin** permite gestionar todos los recursos de impresión: creación de colas, asignación de usuarios a colas, configuración de los puertos, etc.

6. SECUENCIAS DE CONEXIÓN

Las secuencias de conexión son muy importantes para la configuración de los entornos de trabajo de los usuarios de una red y de sistemas multiusuario.

Una secuencia de conexión es una serie de órdenes ejecutadas cuando un usuario entra al sistema. Las órdenes situadas en las secuencias de conexión pueden asignar

unidades de red para los usuarios, situarlos en unidades específicas, mostrar menús e iniciar aplicaciones.

6.1. SECUENCIAS DE CONEXIÓN EN RED

Pueden existir tres tipos de secuencias de conexión, y todas pueden ejecutarse cuando un usuario entra en el sistema:

- Secuencia de conexión del sistema

Está diseñada para establecer el valor de varios parámetros de la red para todos los usuarios. Contiene órdenes que el supervisor cree necesarias para todos los usuarios. Solo el supervisor puede modificarla.

- Secuencia de conexión del usuario

Son específicas de cada usuario. Estas secuencias pueden contener órdenes particulares para el usuario; por ejemplo órdenes que establezcan las asignaciones a directorios, a grupos o a programas que solo necesite el usuario. Los usuarios pueden modificar sus secuencias de conexión.

Cuando un usuario entra al sistema, primero se ejecuta la secuencia de conexión del sistema, a continuación las secuencias de conexión del usuario.

6.2. SECUENCIAS DE CONEXIÓN EN UNIX

Al igual que un sistema en Red, cada vez que un usuario entra en UNIX, se ejecuta una serie de órdenes que personalizan su entorno.

De igual forma se distingue básicamente dos tipos de secuencias de conexión.

- Aquella que afecta a todos los usuarios del sistema.
- La que afecta a cada usuario en particular.

En ambos casos se usa el mismo nombre de fichero, .profile, aunque en directorios diferentes.

7. ENTRADA Y SALIDA DEL SISTEMA

7.1. SISTEMA EN RED

Para entrar en Red se debe ejecutar el comando LOGIN desde la línea de órdenes.

Inmediatamente el sistema nos pedirá nuestro nombre de usuario y nuestra clave de acceso. Es preciso superar esta prueba para acceder a cualquier servicio de red.

Si los datos de identificación son correctos, entraremos al sistema e inmediatamente se ejecutará la secuencia de conexión general para todos los usuarios y posteriormente la secuencial de conexión personal.

De acuerdo con los derechos asignados podremos explorar y utilizar los servicios del servidor.

Para salir de la red podemos ejecutar la orden EXIT o bien LOGOUT.

7.2. SISTEMA MULTIUSUARIO

Para entrar en UNIX hay que identificarse. El usuario debe dar su nombre, aquel que se ha elegido como identificativo (**login**), no es un nombre real sino un alias, normalmente corto, y en minúsculas.

Acto seguido, es necesario dar la contraseña o clave, más conocida como **password**. Si el nombre es identificado, y la clave es correcta, se accede al sistema. Por el contrario, si algo falla, bien el login o el password, aparece Login incorrect.

Para abandonar el sistema, lo habitual es mediante el comando **exit**, o el comando **logout**, o simplemente pulsando **Ctrl-D**.

Hasta aquí el proceso es muy similar al de un sistema en Red.

Sin embargo en UNIX hay un concepto importante: es el de **consolas virtuales**. Se denomina consola del sistema al monitor y al teclado que está conectado directamente. Pero LINUX, al igual que otras versiones UNIX, tienen lo que se denominan consolas virtuales, **VC**, que permiten que un usuario tenga más de una sesión de login al mismo tiempo. Para acceder a una nueva consola virtual se utiliza la combinación de teclas **alt-tecla de función**.

Así para abrir una consola virtual después de haber entrado en el sistema se pulsaría **alt-F2**, y para conmutar a la primera **alt-F1**.

En este caso para abandonar el sistema se deben cerrar todas las sesiones abiertas.

RESUMEN

Las redes locales aparecen como evolución natural de conexión entre el gran número de ordenadores personales. Muchas de las características de los ordenadores personales se han trasladado a la red local.

En una red local podemos utilizar muchos de los comandos del DOS. En un sistema multiusuario, sin embargo, los comandos y utilidades son totalmente distintas.

Es importante tener en cuenta un sistema en red es también un sistema multiusuario.

En el apartado de usuarios la similitud de funcionamiento entre un sistema en Red y un sistema multiusuario es importante. En ambos existe un "superusuario" que tiene todos los derechos o privilegios, usuarios normales y usuarios especiales a los que el "superusuario" les asigna derechos adicionales.

En ambos sistemas la función principal de crear nuevos usuarios en la red es exclusiva del usuario supervisor o root.

Los usuarios de la red necesitan derechos de acceso para acceder a los recursos de la red y para trabajar con los archivos del sistema de archivos. Los derechos determinan exactamente la forma en que el usuario podrá acceder a los directorios y archivos del sistema de archivos.

El único que tiene posibilidad de asignar o cancelar derechos es el usuario supervisor. Algunos de estos derechos pueden ser: Supervisor, Lectura, Escritura, Creación, Borrado.

La orden RIGHTS se utiliza desde el indicador de órdenes para ver o modificar los derechos que los usuarios o grupos poseen sobre archivos y directorios.

En UNIX los permisos se dividen en tres categorías, lectura, escritura y ejecución. Así a cada tipo de usuario (u, g, o) le corresponderá una triada donde se refleje sus privilegios de lectura, escritura y ejecución con respecto a un fichero o un directorio particular.

Para cambiar la cadena de permisos se utiliza el comando **chmod**. Sólo el dueño puede cambiar los permisos de un fichero.

Para un sistema en red la estructura de ficheros y directorios tiene las mismas características que el DOS. Debido a la evolución de la Red a partir del mundo de los ordenadores personales han heredado de estos todas sus características.

En un sistema multiusuario, como es el caso de UNIX, la gestión de archivos y directorios, aunque puede tener grandes similitudes con el DOS (éste es resultado de aquél), nos encontramos con grandes diferencias: tipos de archivos, comandos, las utilidades de que dispone, etc.

Tanto en un sistema en una Red como en un sistema multiusuario la gestión de impresión es muy similar, a través de colas de impresión.

Una secuencia de conexión es una serie de órdenes ejecutadas cuando un usuario entra al sistema. Tanto en red como en UNIX, cuando un usuario accede al sistema se ejecutan diversas secuencias de conexión.

Al igual que en red, para entrar en un sistema multiusuario, todo usuario debe identificarse con su nombre o alias y posteriormente debe especificar su clave personal.

EDITA Y DISTRIBUYE:

CENTRO DOCUMENTACIÓN DE ESTUDIOS Y OPOSICIONES
C/ CARTAGENA, 129 - TELS. 564 39 94 - 28002 MADRID