INTRODUCCIÓN AL SISTEMA OPERATIVO WINDOWS NT

NT hereda las interfaces de usuario desarrollados para la familia Windows. Por ejemplo en las versiones 3.X de NT se utilizan el administrador de programas y demás elementos del Windows 3.X, mientras que en NT 4.0 se emplea el nuevo interface de Windows 95. Esto permite reducir la curva de aprendizaje para el nuevo sistema operativo. NT saca un mejor provecho que los diferentes Windows a la ejecución d e aplicaciones en multitarea real, permitiendo ejecutar varias aplicaciones. simultáneamente, conmutando rápidamente entre ellas.

EJECUCIÓN DE APLICACIONES

NT puede ejecutar varios tipos de aplicaciones:

- *Aplicaciones MSD*OS. La mayor parte de las aplicaciones MSDOS corren sin problemas. Sólo aquellas que acceden directamente a recursos específicos, como pueden ser el puerto serie o el paralelo, o que intentan capturar las interrupciones básicas de MSDOS, no funcionan. Típico ejemplo de estas aplicaciones son las que funcionan con llaves de protección del tipo mochila que no están específicamente preparadas para NT.

- *Aplicaciones Windows de 16 bi*ts. La mayor parte de las aplicaciones de 16 bits funcionan sin problemas bajo Windows NT. Algunas aplicaciones, que utilizan llamadas no documentadas al APIs de Windows, o que hacen suposiciones sobre los recursos de Windows que son sólo válidos en Windows 3.x fallan al ejecutarse sobre NT.

- *Aplicaciones Win*32. Son las nuevas aplicaciones desarrolladas para Windows 95 y NT. Las aplicaciones Win32 eliminan gran parte de los problemas que tenían las aplicaciones Win16, que están basadas en el modelo plano de memoria, que permite a las aplicaciones disponer de hasta 2 gigabytes de datos. Las aplicaciones Win32 se ejecutan siempre como multitarea preemptiva (real), en espacios de memoria separados que evitan que el mal funcionamiento de una de ellas repercuta en las demás. Además las aplicaciones Win32 hacen uso de las nuevas APIs Win32, más potentes y flexibles, con capacidad de ejecución de múltiples hilos. Esto permite a las aplicaciones ejecutar tareas de fondo, como la revisión ortográfica, recálculo, repaginación e impresión típica de los procesadores de texto y de las hojas de cálculo. Esto evita al usuario largos tiempos de espera en su trabajo habitual.

- *Aplicaciones POSIX.* Son aplicaciones basadas en el estándar común POSIX, un subconjunto de las APIs de UNIX. El susbsistema POSIX emula el comportamiento de las aplicaciones UNIX, incluyendo elementos como el uso de enlaces (links) para los ficheros. Para desarrollar aplicaciones POSIX para NT se puede utilizar el compilador que se distribuye en el kit de recursos, o una nueva distribución del popular GCC de GNU (distribución Cignus) que incluye un soporte mucho más

avanzado tanto de aplicaciones Win32 como de aplicaciones POSIX. Este compilador se puede encontrar en los espejos de GNU en la red.

- *Aplicaciones OS/*2. Se pueden ejecutar aplicaciones OS/2 de modo texto. Las aplicaciones basadas en Presentation Manager se pueden ejecutar utilizando un módulo adicional disponible a través de Microsoft..

La red Microsoft Windows

Para ver el funcionamiento de la red Microsoft hay que distinguir dos partes:

- La parte física de la red. El funcionamiento básico de la red Microsoft, basado en el protocolo Netbeui, supone que todos los miembros de la red están interconectados entre sí. Esto implica que no hay barreras del tipo conmutadores o encaminadores de red entre las diversas partes de la red. Cuando aparece este tipo de elementos se utilizan otros protocolos, como el TCP/IP o el IPX, que encapsulan al protocolo Netbeui, permitiendo la integración de la red local dentro de una red más compleja.

- Para la parte lógica de la red, el esquema de red de Microsoft permite trabajar de dos modos diferentes: como grupos de trabajo y como dominios.

LOS GRUPOS DE TRABAJO

En los grupos de trabajos los servidores y estaciones de trabajo configuran una red local del tipo de igual a igual. En este modo de funcionamiento, en principio todos los ordenadores pueden ser clientes y servidores simultáneamente. Los grupos de trabajo fueron introducidos por Microsoft cuando introdujo en el mercado Windows para Trabajo en Grupo. Este esquema de funcionamiento es bastante sencillo, ya que no precisa de la existencia de la figura del administrador del grupo.

Todos los ordenadores a priori se comportan de la misma forma, pudiendo acceder todos ellos a los demás ordenadores de la red. Esto no impide que dentro de un grupo de trabajo se puedan introducir máquinas configuradas exclusivamente como clientes o como servidores.

LOS DOMINIOS NT

El sistema de dominios en NT hereda la funcionalidad que permitía obtener los dominios Lan Manager de Microsoft. El esquema de dominios aporta grandes ventajas en la seguridad de la red,

aunque añade mayor carga administrativa. En un grupo de trabajo, al no existir la figura del administrador, deben ser los propios usuarios los que se encar guen de la configuración de la seguridad. El sistema de dominios introduce la figura del administrador. Éste es el responsable de mantener la seguridad del dominio, dando de alta a los usuarios y asignándoles privilegios de acceso a los recursos del dominio.

Un dominio está compuesto por al menos un controlador primario del dominio y por estaciones de trabajo que actúan como clientes del dominio. El controlador principal del dominio va a ser el ordenador que va a almacenar la base de datos de usuarios y de ordenadores del dominio. Un dominio puede tener varios tipos de clientes:

ð Clientes Windows para trabajo en Grupo, Windows 95, Windows NT Workstation y Server.

ð Ordenadores con Msdos o Windows 3.1, con el cliente de red Microsoft instalado.

ð Ordenadores con OS/2 o Macintosh

ð Otros tipos de ordenadores, por ejemplo los que usan LAN Manager para UNIX, o con el software de SMB (por ejemplo Samba)

USO DE LOS DOMINIOS DE NT

El sistema de dominios introduce una mayor carga administrativa sobre el sistema de grupos de trabajo cuando la red es pequeña. El sistema de dominios necesita una mayor planificación inicial frente al grupo de trabajo, ya que el administrador debe dar de alta a los usuarios y equipos..

Sin embargo, al ampliar la red esa mayor carga administrativa inicial se traduce en una mayor simplicidad de la administración de una red corporativa. Cuando el número de ordenadores y de usuarios de la red comienza a superar las decenas, la estructura creada por el dominio aporta numerosas ventajas. La primera y más importante es la seguridad del dominio. En un dominio la base de datos de usuarios y de equipos es única, y está centralizada. A cada usuario se le asigna una cuenta que le identifica en el dominio. En principio la autenticidad del usuario está garantizada por el uso de su contraseña. Esto facilita al usuario el acceso a los recursos del dominio, ya que la mayor parte de las veces no necesitará introducir su contraseña. El esquema de dominios permite además

crear grupos de usuarios. Los grupos de usuarios facilitan la administración de los dominios ya que permite asignar seguridad, aplicaciones y otros recursos del dominio a grupos de usuarios con características comunes. El sistema de grupos de usuarios es muy flexible, permitiendo adaptar el dominio a la estructura corporativa. Un usuario del dominio puede pertenecer a varios grupos, de manera que cada uno de los grupos a los que pertenece le permita realizar una serie de tareas diferentes.

El sistema de dominios simplifica la administración de servidores y estaciones de trabajo. A medida que se añaden estaciones y servidores al dominio, el administrador utiliza las herramientas administrativas para darlos de alta en el dominio. Cuando un equipo es dado de alta en el dominio puede comunicarse de una manera segura con los demás miembros del dominio. De esta manera puede reconocer a los demás usuarios y equipos del dominio.

Esta tarea es realmente sencilla. Durante el proceso de instalación de una estación de trabajo o servidor NT, aparece un cuadro de diálogo en el que se da la oportunidad de añadir el equipo al dominio. Para añadir el equipo basta escribir el nombre del dominio y nombre de usuario y contraseña con privilegios de administrador válido en el dominio. El proceso de instalación se pone en contacto con el controlador del dominio y da de alta al ordenador en el dominio. Una vez que se ha dado de alta en el dominio, el programa de instalación configura automáticamente el sistema para que sea miembro del dominio. El proceso completo se desarrolla en pocos segundos y sin intervención del usuario.

El sistema de dominios simplifica enormemente la gestión de grandes dominios, ya que los cambios introducidos en la configuración del dominio se reflejan automáticamente en todos los miembros del dominio. Si por ejemplo se añade un nuevo equipo al dominio, queda disponible para el uso por los demás miembros del dominio.

ELEMENTOS DE UN DOMINIO

En un dominio se pueden integrar varios tipos de servidores y de clientes. En todo dominio puede haber:

ð *Un controlador principal del domin*io. Es obligatorio, ya que es el equipo que mantiene la base de datos

del dominio. Este servidor debe ser obligatoriamente un NT Server configurado como controlador principal del dominio.

ð *Controladores de reserva del domin*io. Puede haber varios en el dominio. Su labor consiste en ayudar al controlador principal en caso de sobrecarga o mal funcionamiento de éste. Es recomendable siempre tener al menos un controlador de reserva correctamente configurado, ya que de este modo se asegura que siempre los usuarios podrán iniciar sesión correctamente en el dominio.

ð *Estaciones de traba*jo. Son los clientes del dominio, y pueden ser de diferentes tipos (Windows, Os/2, etc.)

ð *Servidores* NT. Se puede configurar NT Server en el modo servidor. En este modo, el servidor no colabora en la validación de los inicios de sesión por parte de los usuarios, con lo que la carga del servidor es menor. Este modo se suele utilizar para configurar servidores de ficheros y aplicaciones, como servidores SQL y de Internet. Además, un NT Server configurado como servidor mantiene su propia base de datos, además de poder acceder a la del dominio. Esto permite tener cuentas separadas de las del dominio. El uso fundamental que se puede dar a esta funcionalidad consiste en crear grupos de usuarios ajenos al dominio, que se pueden eliminar fácilmente sin más que eliminar el servidor.

ð *Otros tipos de servidores.* Hay varios sistemas operativos que de alguna forma pueden acceder al dominio NT, normalmente con sus propias herramientas de integración. Por ejemplo, desde que Microsoft hizo público el protocolo SMB, hay sistemas que soportan parte de la funcionalidad de este protocolo, aunque no se pueden construir controladores de dominio con otros sistemas operativos.

EL SISTEMA DE RECURSOS DE RED

En una red Microsoft se pueden compartir varios tipos de recursos, como pueden ser impresoras y unidades de red. En una red Microsoft el nombre de los recursos sigue el siguiente convenio:

\\servidor\recurso

escrito en el formato UNC (Universal Name Convention). Servidor es el nombre del servidor que

comparte el recurso. Recurso es el nombre que se le da al recurso. En el caso de recursos del tipo unidad de red, detrás del nombre de recurso se puede poner la ruta completa de directorios, y el nombre de un archivo cuando nos estamos refiriendo a un archivo remoto, de este modo:

\\servidor\recurso\directorio\directorio\fichero.extension

Además de poder compartir unidades de disco e impresoras, se pueden compartir otro tipo de recursos, como unidades CD−ROM, módems, fax (con el software adecuado, no incluido en NT), y otros tipos de recursos especiales, como pueden ser las tuberías creadas entre el controlador del dominio y los ordenadores conectados a él.

Para crear los recursos se deben utilizar las herramientas apropiadas en cada caso:

ð Para unidades de red, se utiliza el explorador de Windows NT, o el administrador de archivos (Winfile.exe)

ð Para compartir impresoras se utiliza el administrador de impresión.

ð Para tipos especiales de recursos, normalmente hay herramientas especiales que lo hacen.

Normalmente todos los recursos compartidos aparecen en los listados de recursos de red de todos los clientes. Se puede modificar el nombre de recurso para que no aparezca en los listados de recursos. A este tipo de recursos se les llama recursos compartidos en modo administrativo. Para compartir un recurso en modo administrativo basta con añadir un signo $ al final del nombre de recurso:

\\servidor\nombre$

Por ejemplo, siempre que se inicia NT, el sistema de red comparte automáticamente en modo administrativo las unidades de disco. Así por ejemplo tendremos:

\\servidor\c$

\\servidor\d$.

compartidas automáticamente al arrancar el ordenador. Luego se pueden dejar de compartir, si fuese necesario. Además NT añade los permisos correspondientes para que sólo tengan acceso los administradores. Para ver los recursos compartidos en modo administrativo se puede:

- Abrir el Panel de Control, en el icono Servidor, y ver los recursos compartidos.
- Abrir el Administrador de Servidores de NT Server, y seleccionando un servidor o estación de trabajo, ver los recursos compartidos.

- Este mecanismo permite de una manera muy cómoda acceder a los administradores a los diferentes discos de todas las estaciones de trabajo del dominio, para realizar labores de copia de ficheros, instalación de aplicaciones, y otras tareas.

Para conectarse a un recurso compartido en modo administrativo, ya que su nombre no aparece en los listados de recursos, debemos seleccionarlo manualmente:

- Escribiendo su nombre directamente, en el cuadro de diálogo Conectarse a una unidad de red.

- Utilizando NET USE \\servidor\recurso$ letra:

INICIO DE SESIÓN EN UN GRUPO DE TRABAJO

Cuando un usuario va a acceder a una red, lo primero que debe realizar es un inicio de sesión. El inicio de sesión consiste en que el usuario debe introducir un nombre de usuario y una contraseña, que serán utilizados por el sistema para acceder a la red. Ya que en el grupo de trabajo no hay servidores dedicados a validar los inicios de sesión, el inicio de sesión en Windows para trabajo en grupo es simple. El inicio de sesión es un mero anuncio de que el usuario se dispone a utilizar los recursos de red. No se realiza ninguna comprobación de seguridad, es decir, cualquier usuario puede iniciar sesión con cualquier nombre dentro del grupo de trabajo. No existe ningún mecanismo que impida al usuario iniciar sesión de red.

Durante el inicio de sesión en un grupo de trabajo, al usuario se le pide su nombre de usuario y su contraseña. En Windows para Trabajo en Grupo el nombre de usuario se utiliza como identificador del usuario, aunque no hay ninguna garantía de la verdadera identidad del usuario. La contraseña facilitada por el usuario se utiliza para dos tareas:

- Cuando se acceden a los recursos de red protegidos por contraseña, Windows para Trabajo en Grupo facilita esta contraseña en primer lugar. Si la contraseña no es válida, mediante un cuadro de diálogo se pedirá al usuario la contraseña correcta para acceder al recurso.

- La contraseña además se utiliza para encriptar el archivo de contraseñas, que normalmente se llamará nombre.pwl, donde nombre es el nombre del usuario. En este archivo se guardan las contraseñas utilizadas por el usuario para acceder a los recursos de red. Si un usuario ha olvidado la contraseña, no podrá desbloquear el archivo de contraseñas.

Normalmente puede iniciar sesión con otro nombre de usuario, y borrar el antiguo archivo de contraseñas, con lo que de nuevo podrá iniciar sesión en el sistema con su nombre de usuario habitual.

El esquema de contraseñas de los grupos de trabajo suele ser bastante engorroso, ya que cuando la contraseña de un recurso cambia obliga a difundir de nuevo las contraseñas a los usuarios interesados. Además los archivos de contraseñas son muy fáciles de desbloquear, existiendo en Internet numerosas utilidades que lo hacen.

Windows para trabajo en grupo es bastante difícil de cerrar, para impedir el acceso al sistema y a la red de un usuario que no tiene permiso para ello..

INICIO DE SESIÓN EN UN DOMINIO

Aparentemente el método de inicio de sesión en un dominio NT es similar al utilizado en un grupo de trabajo. El usuario tiene que realizar el proceso de inicio de sesión o logon, suministrando un nombre de usuario y una contraseña válida para el dominio.

El proceso de inicio de sesión en un dominio es más sofisticado:

- El usuario proporciona el nombre de usuario y la contraseña en el cliente del dominio.

Dependiendo del cliente, este procedimiento puede ser más o menos seguro. Por ejemplo, en Windows para trabajo en grupo se siguen los mismos pasos que para el inicio de sesión de red normal, aunque la contraseña para el dominio hay que proporcionarla en un cuadro de diálogo separado, para mayor seguridad. En Windows NT, el proceso de inicio de sesión automáticamente registra al usuario en el dominio, y requiere el uso de una combinación especial de teclas: Ctrl+Alt+Suprimir.

- El cliente solicita el inicio de sesión al servidor controlador del dominio. En este momento el

servidor envía al cliente un conjunto de datos. Este esquema de validación es un esquema de tipo *desafío/respues*ta.

- El cliente encripta los datos enviados por el servidor con la contraseña que le ha suministrado el usuario. Este nuevo conjunto de datos es enviado al servidor.
- El servidor encripta los datos originales, con la contraseña del usuario que guarda en la base de datos de NT. Ahora compara ambos conjuntos de datos.
- Si los datos codificados por el servidor y por el cliente coinciden, el servidor valida al usuario para acceder al dominio.

Durante el proceso de inicio de sesión, la contraseña del usuario no viaja por la red, ya que con el sistema de reto, lo que viajan son paquetes de datos codificados, pero no la contraseña que los codifica. Este sistema tiene un punto vulnerable, ya que en el servidor se almacenan las contraseñas de todos los usuarios en la base de datos de usuarios. Sin embargo, se han introducido mejoras en el sistema de gestión de la base de datos, que hace muy difícil el acceso a las contraseñas incluso para los propios administradores de NT. Estas mejoras fueron introducidas con el Service Pack 3 para NT Server.

El inicio de sesión en el dominio sólo se produce una vez. Es decir, una vez que un usuario ha iniciado sesión en un dominio, no necesita suministrar de nuevo su contraseña para acceder a los diferentes recursos del dominio. En todo momento, la validación del usuario se va a realizar a través de los controladores y servidores.

El sistema de seguridad de NT no sólo permite gestionar el acceso de los usuarios a los recursos, sino que incluso se pueden crear grupos de usuarios a los que se les asignan privilegios, por lo que la gestión de la seguridad se simplifica dentro del dominio.

LOS CONTROLADORES DEL DOMINO

Todo dominio tiene una base de datos de usuarios. La copia original de esta base de datos reside en el controlador principal del dominio. En esta base de datos quedan registradas todas las características de los usuarios, sus cuentas, y de los ordenadores que forman parte del dominio.

Además del controlador principal del dominio, puede haber dentro de un dominio varios controladores secundarios del dominio. En estos controladores se mantiene una copia de la base de datos de usuarios del dominio. Si el controlador del dominio está muy cargado o simplemente está inactivo, cualquier controlador del dominio puede validar el inicio de sesión en el dominio.

El proceso de inicio de sesión en los controladores del dominio comienza en el cliente por obtener la lista de controladores del dominio. Para ello el servicio Examinador de computadoras, obtiene dicha lista, bien mediante una pregunta por difusión (broadcast), o bien preguntando a los servidores WINS del dominio. Una vez obtenida la lista, el cliente envía una petición de inicio de sesión a los diferentes controladores del dominio. El cliente elegirá al primer controlador de dominio que le conteste para intentar el proceso de inicio de sesión. Este método asegura que siempre el cliente pueda iniciar sesión en el dominio.

El mantenimiento de la base de datos del dominio es automático. Las herramientas administrativas de NT permiten modificar la base de datos, mediante el Administrador de usuarios para dominios. Los cambios se realizan siempre sobre el controlador principal del dominio, y son enviados automáticamente a los demás controladores del dominio. Hay que tener en cuenta que esto se realiza con una pequeña demora temporal, que se puede reducir sincronizando los servidores con el administrador de servidores.

DIFERENCIAS ENTRE NT WORKSTATION Y NT SERVER

El sistema operativo Windows NT se comercializa en dos versiones: Workstation y Server. La versión Workstation está pensada para configurar puestos de trabajo, donde se ejecutarán las aplicaciones de usuarios. NT Workstation es una plataforma que incluye todos los elementos para trabajar con aplicaciones Windows y para trabajar en red. Incluye una pila completa TCP/IP. NT Server está preparado para configurar servidores. Aunque realmente los núcleos de NT Server y Workstation son muy parecidos, la versión Server incluye una serie de mejoras en el núcleo y en los diferentes módulos del sistema que lo hacen más robusto en tareas de servidor de red. NT Server da mayor prioridad a los accesos mediante red frente a las aplicaciones de usuario que se

ejecutan en el servidor. Además NT Server no tiene el límite de 10 conexiones simultaneas de red que tiene NT Workstation. NT Server ofrece mayor seguridad en el almacenamiento de datos, ya que posee características avanzadas de tolerancia a fallos que no han sido incluidas en la versión Workstation.

AGREGAR O QUITAR PROGRAMAS

En este icono podemos acceder a un cuadro de diálogo que nos permite realizar varias labores:

- *instalar nuevas aplicacion*es. El botón instalar lanza un asistente que busca en las unidades de disco y de CD−ROM ficheros con nombre típico de programas de instalación , como pueden ser instalar.exe y setup.exe y si los encuentra nos permite ejecutarlos.

- *eliminar los programas instalados.* Muchos programas para Windows 95 y NT traen sus propios programas de desinstalación automática. Estos programas saben como registrarse en el registro de NT, de manera que pulsando el botón de agregar o quitar se reinstalan o desinstalan automáticamente.

- *instalar o eliminar componentes adicionales de* NT. Durante el proceso de instalación, al elegir una de las posibles instalaciones (típica, portátil, a medida...) se seleccionan los componentes que se han de instalar. Con este cuadro de diálogo podemos añadir o eliminar componentes adicionales desde el CD−ROM de instalación.

DESINSTALACIÓN MANUAL DE APLICACIONES

Ocurre a veces que el programa de instalación de una aplicación no es capaz de desinstalarla.

Esto puede ocurrir por un fallo del propio programa o porque otra aplicación la ha alterado. En este caso se debe proceder manualmente. Para ello:

- se deben eliminar todos los ficheros de la aplicación. Normalmente hay que borrar el directorio de la aplicación y algunos directorios de datos.

- se deben borrar los accesos directos creados por la aplicación. Esto se puede hacer con el explorador de NT, en el escritorio y en el menú de inicio.

- se deben borrar las librerías de haya dejado la aplicación en el sistema. En NT y 95 al instalar una librería se incrementa la clave del registro:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SharedDlls

correspondiente a la librería

- se deben eliminar las claves del registro que ha añadido la aplicación, normalmente en: HKEY_LOCAL_MACHINE\Software\Compañía\Aplicación y en otras partes del registro. La clave del registro:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

Indica el nombre del programa de desinstalación para la aplicación..

CONFIGURACIÓN REGIONAL

NT, al igual que Windows, está preparado para soportar diversos idiomas y trabajar en diferentes países, con diferentes esquemas de ordenación alfabética, moneda y formas de escribir la fecha, hora y signos de puntuación en números y monedas. Se puede modificar:

ð Configuración regional: Permite seleccionar las características del idioma de cada región.

ð Número. Selecciona el formato para números y el sistema de medida.

ð Moneda. Selecciona la representación de cantidades monetarias.

ð Hora: Selecciona el formato para representar las horas

ð Fecha: Selecciona el formato para representar las fechas.

ð Idioma. Permite seleccionar y añadir diferentes idiomas, con sus correspondientes configuraciones de teclado. También permite habilitar atajos del teclado que intercambian las configuraciones del teclado.

CONSOLA

El cuadro de diálogo Consola configura las opciones del subsistema MSDOS, esto es, normalmente lo que aparece en la ventana MSDOS..

Podemos configurar muchas opciones:

ð Tamaño del cursor en la ventana, de la ventana, historial de comandos y los modos de inserción y pegado rápido (emula el comando DOSKEY de DOS).

ð Tipo de letra para la ventana MSDOS.

ð Tamaño de la ventana y del buffer de la ventana.

ð Colores del texto, fondo y otras ventanas dentro de la ventana DOS.

IMPRESORAS

Normalmente la mayoría de las aplicaciones ofimáticas necesitan una impresora predeterminada para funcionar. Para instalar una nueva impresora al sistema NT dispone de un sencillo asistente que nos guía en el proceso de instalación. Para acceder a este asistente se utiliza el icono Agregar impresora del Panel de control\Impresoras.

En NT la impresora puede estar instalada en el propio equipo o ser una impresora de red. El caso más sencillo consiste en que la impresora esté conectada a un servidor NT, que la ha compartido. En este caso para conectarnos a la impresora basta seleccionar en el asistente la opción *Servidor de impresora de red.* Al seleccionar esta opción aparece un cuadro de diálogo con las impresoras compartidas por los equipos. Las impresoras compartidas por los NT aparecen aparte, como elementos separados del equipo que las comparte, haciendo más fácil su localización. La opción instalar la impresora en el propio equipo conduce a una serie de asistentes que nos permiten configurar y compartir la impresora.

El primer paso consiste en seleccionar el puerto al que está conectada la impresora. Puede ser:

ð Un puerto paralelo LPT, normalmente el LPT1

ð Un puerto serie (los trazadores gráficos antiguos los suelen usar).

ð Un puerto de red (cuando hay conexiones a impresoras de red)

ð Un archivo. En este archivo se almacenarán los comandos necesarios para imprimir el documento en la impresora. Se suele usar para generar archivos Postcript.

ð Un puerto nuevo, que quizás usa un hardware o software especial. Un ejemplo de este tipo son los puertos Jetdirect de red usados por las impresoras HP.

En este cuadro de diálogo se puede activar la cola de impresión de NT (normalmente esta opción no se activa por defecto, sino que se imprime directamente en el puerto)

Luego hay que elegir el modelo de la Impresora. El cuadro de diálogo está organizado por Fabricantes y modelos, por lo que se encuentran rápidamente los modelos adecuados. También se

puede añadir una impresora no disponible en NT con los controladores porporcionados por el fabricante.

Tras elegir el modelo hay que ponerle un nombre en el siguiente cuadro de diálogo.

Normalmente NT elige un nombre adecuado, que coincide con el modelo de la impresora..

El siguiente cuadro de diálogo permite compartir la impresora. Si se comparte NT se debe elegir:

ð Un nombre para la impresora, que también sugiere el asistente.

ð Los controladores que se van a compartir. Se puede añadir el soporte para otras plataformas NT y Windows, aunque hará falta tener los discos correspondientes. Esto permite que los clientes se conecten a nuestra impresora sin necesidad de instalar ellos ningún controlador de impresora. Al conectarse a la impresora los controladores se transfieren al cliente de forma automática.

ð El proceso de instalación finaliza con la impresión de una página de prueba opcional, que permite verificar la correcta instalación de la impresora.

EL ADMINISTRADOR DE IMPRESIÓN

El antiguo administrador de impresión de Windows 3.X y NT se ha sustituido por la Carpeta de Impresoras, que es accesible desde el Panel de Control o desde el menú de Inicio, en el menú de configuración. Con la nueva carpeta de impresoras podemos:

ð Abrir el asistente para añadir una nueva impresora.

ð Abrir la cola de impresión de una impresora, configurar la impresora y compartirla.

ð Conectarnos a un servidor de impresión para configurarlo.

ð Conectarnos a una impresora de red.

En la carpeta de impresoras aparecerá un icono que permite acceder a la impresora. La ventana de control de la impresora muestra los documentos que se están imprimiendo y permite además acceder a todas las opciones de configuración de la impresora..

El menú Impresora tiene varias opciones:

ð Pausa impresión. Permite detener la impresión de los documentos.

ð Establecer como predeterminada. En el sistema sólo puede haber una impresora predeterminada,

qe será la que usen las aplicaciones por defecto.

ð Valores predeterminados del documento. Cuando se crea un documento normalmente la aplicación configura el documento con los parámetros por defecto de la impresora. Normalmente las aplicaciones luego permiten modificar estos parámetros.

ð Compartir. Permite compartir o modificar las opciones utilizadas para compartir la impresora.

ð Propiedades. Permite acceder a una serie de cuadros de diálogo para compartir la impresora.

El menú Impresora\propiedades permite acceder al cuadro de diálogo de configuración de la impresora. Este cuadro de diálogo está formado por una serie de pestañas:

ð General. Permite modificar el nombre, modelo y comentario de la impresora. También se puede especificar aquí el controlador para la impresora, así como el procesador de impresión utilizado.

ð **Configuración del dispositivo.** Accede a las opciones de impresión de la impresora, como color, tipo de papel, tipos de letra instalados y otras. Depende del modelo de impresora instalada.

ð **Plan de impresión.** Permite configurar algunas opciones de la cola de impresión que permiten una mayor agilidad en la impresión de documentos

ð **Puertos.** Permite modificar el puerto al que se ha conectado la impresora, así como activar y desactivar la cola de impresión..

ð **Seguridad.** Permite configurar las opciones de seguridad y auditoria de la impresora. Serán explicadas en el capítulo dedicado a seguridad.

ð **Compartir.** Mediante este cuadro de diálogo se puede compartir de modo sencillo la impresora en red. Al compartirla hay que asignarle un nombre de recurso. Además se pueden compartir los controladores necesarios para que otros usuarios utilicen la impresora sin necesidad de instalar controladores en su equipo.

ð **Propiedades predeterminadas del documento.** Este cuadro de diálogo está dividido en dos pestañas. La primera nos permite configurar las opciones más sencillas:

− Tamaño del papel

− Origen del papel, para impresoras con varias fuentes de papel, (bandejas, carga manual

del papel, sobres, etc.)

− Orientación de la impresión: vertical, horizontal (apaisada), o invertida (rotada)

− Número de copias.

− Impresión por ambos lados, para impresoras que lo soportan.

− Color, para las impresoras en color y grises..

ð **Opciones avanzad**as. Permiten configurar gran cantidad de opciones:

− Opciones del papel, como orientación y tipo de papel empleado.

− Opciones de impresión de los gráficos, para seleccionar la calidad y apariencia de los gráficos.

− Opciones del documento, como ajustes de los medios tonos o calidad de impresión.

CONEXIÓN A UN SERVIDOR DE IMPRESIÓN.

Cuando nos conectamos como administradores a un servidor de impresión podemos configurarlo remotamente, del mismo modo en que se hace con las impresoras locales. Se puede compartir las impresoras del servidor o estación de trabajo NT y configurar las impresoras. También se puede acceder a las colas de impresión para gestionar los documentos que se están imprimiendo.

El cuadro formularios permite definir los diferentes tamaños de papel soportados por la impresora. NT define los más habituales por defecto..

El cuadro de diálogo avanzadas permite asignar algunas propiedades avanzadas del servidor de impresión. La más importante es el directorio donde se almacena la cola de impresión. Hay que recordar que en este directorio se suelen almacenar ficheros intermedios de gran tamaño. Este directorio normalmente reside en la partición del sistema, por lo que se puede llegar a desbordar el sistema.

El cuadro de puertos permite ver los puertos en los que se puede imprimir, así como añadir, eliminar y configurar los puertos..

INTERNET

El cuadro de diálogo Internet ha sido incluido para ajustar algunas opciones de los navegadores de Internet, en especial las opciones del Internet Explorer.

MODEMS

Este cuadro de diálogo permite instalar y configurar los módems. Es muy sencillo de utiliza, aunque conviene tener en cuenta algunos detalles. El proceso de instalación es sencillo. El asistente de instalación busca en todos los puertos COM la presencia de un módem. Cuando encuentra un módem permite lo configura correctamente si lo reconoce o pide al usuario que le asigne una configuración. Los modem que siguen la norma Plug and Play se instalan también de esta forma, pero hay que instalar primero el controlador ISA Plug and Play, que se halla en el disco de NT, en el directorio de drivers. Una vez instalado este controlador, al añadir un módem y arrancar el sistema, NT lo reconoce y configura o pide el controlador correspondiente..

Una vez configurado el módem, el cuadro de diálogo muestra una lista de los módems instalados y de las propiedades de marcado activas.

ADAPTADORES SCSI

En este cuadro de diálogo se pueden ver tanto los dispositivos SCSI añadidos al sistema como los controladores de dispositivo (drivers) SCSI instalados.

En la pestaña de dispositivos vemos la lista de dispositivos SCSI, organizada por controladores SCSI. En la pestaña controladores aparece la lista de controladores de dispositivo SCSI.

Nota: En la versión 3.51 de NT esto aparecía en el icono Instalación de Windows NT. Para añadir un controlador SCSI al sistema, se pulsa el botón agregar de la pestaña controladores. Si el controlador no aparece en la lista se puede insertar uno con un disco del fabricante. El programa de instalación también permite detectar el adaptador SCSI instalado.

Una vez añadido el controlador SCSI, en este cuadro de diálogo aparecen todos los dispositivos SCSI conectados a cada adaptador.

DISPOSITIVOS

Este cuadro de diálogo permite ver el estado de los dispositivos instalados en el sistema. NT por defecto instala gran cantidad de dispositivos aunque no los utilice. En particular, el programa de instalación de NT carga los controladores SCSI y algunos controladores de dispositivos de pantalla.

Esto es necesario ya que durante el proceso de instalación se puede pedir a NT que busque estos dispositivos. Para ello NT carga cada controlador de dispositivos e intenta iniciarlo. Si el controlador de dispositivo arranca quiere decir que el dispositivo está funcionando correctamente..

Cada dispositivo puede tener:

ð **Un tipo de inicio.**

ð *Inic*io. Se utiliza para controladores de dispositivos que se cargan en las primeras etapas de carga del sistema, como por ejemplo el controlador ATAPI y el DISK.

ð *Siste*ma. Son los dispositivos que se cargan después de cargar el sistema. Por ejemplo el controlador del ratón y de la disquetera (floppy)

ð *Automático.* Estos dispositivos se cargan de la carga completa del sistema.

ð *Manua*l. Estos dispositivos los carga el usuario u otros controladores de dispositivos. Por ejemplo el controlador de la tarjeta de red normalmente lo carga los servicios de red.

ð *Deshabilita*do. Son controladores de dispositivos que no se pueden cargar normalmente, como por ejemplo los controladores SCSI de adaptadores no instalados. Hay algunos dispositivos que aparecen como deshabilitados pero están iniciados. Estos dispositivos se cargan en la primera fase de arranque del sistema operativo. Por eje mplo los controladores de sistemas de ficheros FastFAT y NTFS son un ejemplo.

ð **Un estado.** El dispositivo puede estar iniciado o no iniciado.

ð **Un perfil asociado**. NT permite definir perfiles del sistema diferentes. Cada perfil tiene su propia configuración del sistema. Normalmente se usa para equipos portátiles con unidades de expansión de puertos (docking stations), que permiten añadir periféricos al portátil al insertar el portátil en la ranura de expansión.

DISPOSITIVOS DE CINTA

Este cuadro de diálogo permite agregar dispositivos de cinta. El funcionamiento es análogo al de Adaptadores SCSI, aunque se ha incluido un botón para detectar los dispositivos de cinta instalado.

LICENCIAS

Este cuadro de diálogo permite ver las licencias adquiridas de productos. En general se utiliza para los productos del Backoffice, como son el propio NT y los servidores SQL, SNA, etc. de Microsoft.

RED

En el icono de Red se pueden configurar los elementos de la red. Está organizado en una serie de pestañas:

− Identificación de la máquina

− Servicios de red

− Protocolos de red.

− Adaptadores de red

− Enlaces.

ð **Identificación de la máquina.** Esta pestaña permite cambiar el nombre del equipo y el grupo de trabajo o dominio al que pertenece el equipo. Como siempre, el nombre del equipo debe ser único dentro de la red Microsoft Windows en que se halle el equipo, independientemente de los grupos de trabajo y dominios que se halen definidos. Un equipo con NT se puede añadir de un modo sencillo a un grupo de trabajo o un dominio NT:

ð *Para añadir a un grupo de trabajo* sólo hay que pulsar el botón ***Cambiar*** y en el cuadro de diálogo introducir el nuevo nombre del grupo de trabajo. No existe ninguna restricción para añadir el equipo (salvo que el número de equipos en el grupo de trabajo no puede ser mayor de unos 250), ya que en los grupos de trabajo no existe sistema de seguridad que compruebe la validez de un equipo..

ð *Para añadir el equipo a un domin*io, el administrador primero debe crear una cuenta para el equipo. Esto no es necesario si el usuario que quiere añadir el equipo tiene privilegios de administrador en el dominio. En este caso puede crear la cuenta para el equipo y añadirlo al dominio en un solo paso, escribiendo su nombre de usuario y contraseña en el dominio. En este momento el equipo se pondrá en contacto con el controlador primario del dominio para darse de alta en él. El mensaje de

bienvenida al dominio indica que la operación se ha realizado con éxito.

ð **Adaptadores**. Se pueden instalar fácilmente nuevos adaptadores en el equipo. NT crea una lista clasificada por marcas y modelos, o permite introducir uno desde un disco o directorio. En el caso de no disponer de ninguno se puede instalar para hacer pruebas el Microsoft Loopback, que no necesita adaptador físico.

ð **Protocolo**s. Esta pestaña permite añadir nuevos protocolos para pilas de red. Algunas de las soportadas por NT son:

ð *Protocolo TCP/*IP, Es el principal protocolo de Internet y de entornos UNIX..

ð *Protocolo Netbe*ui, Utilizado en entornos Microsoft e IBM.

ð *Protocolo IPX/S*PX, utilizador en entornos Novell.

ð *Protocolo AppleTa*lk, utilizado en entornos McIntosh.

ð *Protocolo D*LC, utilizado para conectividad con entornos tipo Mainframe tipo AS/400 y para impresoras de red tipo HP Jectdirect.

ð *Point to Point Tunneling Protoco*l, que permite crear redes privadas virtuales sobre una red pública.

El botón ***Agregar nuevo protocolo*** permite obtener una lista de protocolos, transportes y entornos soportados.

ð **Servicios.** Muchos de los elementos de red se instalan en NT como servicios. Esta pestaña permite instalar y configurar los servicios de red. Algunos de los más importantes son:

ð **Estación de trabajo.** Este es el módulo cliente en la red Microsoft.

ð **Servidor.** Este es el módulo servidor en la red Microsoft.

ð **Examinador de equipos.** Este servicio es el responsable de obtener los nombres de red Windows de los demás equipos. Es utilizado por el interfaz Netbios.

ð **Interfaz Netbi**os. Este servicio proporciona todos los servicios de red dentro de la red Windows, como puede ser compartir ficheros e impresoras, mensajería Windows y otros.

ð **Configuración de R**PC. Se utiliza para que el sistema realice las llamadas a procedimientos remotos. Las herramientas administrativas de NT utilizan estas llamadas para configurar los equipos

remotos.

ð **Microsoft Information Server.** Es el servidor Web, FTP y Gopher de Microsoft. El servidor IIS tiene sus propias herramientas de configuración y administración separadas.

· · **Servicios de TCP/IP simples.**

ð **Enlaces.** Esta pestaña permite ver los enlaces que se generan entre adaptadores, protocolos y servicios. NT por defecto activa todos los enlaces soportados, aunque aveces es necesario desactivar algunos . Por ejemplo, se pueden activar protocolos diferentes para cada adaptador de red instalado en el equipo. Esta situación se suele producir cuando cada adaptador está conectado a un tipo de red diferente.

SERVICIOS

En NT las aplicaciones que se ejecutan independientemente de las sesiones interactivas de los usuarios se llaman servicios. Los servicios de NT son equivalentes a los demonios de otros sistemas operativos como UNIX. Un servicio puede constar de un proceso, o incluso un único proceso puede manejar varios servicios, dependiendo de cómo se haya programado. El sistema de gestión de servicios de NT está formado por un cuadro de diálogo que permite ver el estado de todos los servicios que se han instalado en el sistema, así como configurarlos e iniciarlos. Los servicios de NT se benefician de una serie de procedimientos en las APIs de NT, que permiten a los programadores utilizar una interfase de gestión común para todos los servicios.

Todos los servicios poseen una serie de características comunes, que pueden ser controladas con el cuadro de diálogo Servicios:

ð Estado del servicio. Un servicio puede estar iniciado, en pausa o no iniciado. Se puede iniciar un servicio pulsando el botón de inicio, o mediante el comando NET START.

ð **Tipo de inic**io. Cada servicio tiene uno de los siguientes posibles tipos de inicio:

ð *Desactivado.* Se utiliza para no permitir el arranque de un servicio. Por ejemplo, si no deseamos que los usuarios puedan utilizar los servicios DFDE de red (Intercambio dinámico de datos en red), basta con desactivar el servicio.

ð *Manual.* Estos servicios suelen iniciarse por una acción del usuario o por la acción de otra aplicación o servicio. Normalmente la aplicación suele detener el servicio cuando no lo necesita.

ð *Automático.* Los servicios automáticos se inician tras la carga del sistema operativo, para que puedan ser usados por las aplicaciones. Por ejemplo el servicio Servidor, encargado de ofrecer los servicios de ficheros e impresoras, se inicia automáticamente, independientemente de que el usuario haya o no iniciado sesión de red..

ð **Cuenta de inicio.** Todo servicio tiene asociado una cuenta con la que se ejecuta. El servicio posee las limitaciones de la cuenta con la que se inicia. Hay dos tipos principales de servicios: los que se inician con la cuenta del sistema operativo (NT tiene una cuenta que identifica al sistema operativo), y los que se inician con otra cuenta. Hay que hacer notar que la cuenta del sistema tiene una importante limitación: no tiene acceso a la red. Esto debe ser tenido en cuenta si el servicio debe acceder a ficheros que están en otro ordenador de la red. El ejemplo más sencillo es el servidor Web IIS, que permite incluir en el árbol de directorios a directorios que residen en otros servidores. En este caso el servidor Web realiza un inicio de sesión local o como proceso por lotes en uno de sus hilos para acceder a los ficheros en el otro ordenador, ya que este servicio se inicia con la cuenta del sistema. Si indicamos que el servicio se va a iniciar con otra cuenta, debemos suministrar en este cuadro de diálogo el nombre de usuario y la contraseña. Si la contraseña se modifica, el servicio no se puede iniciar Además, se puede impedir que un servicio puede acceder al escritorio (entorno del usuario).

ð **Perfil de Hardware.** En ordenadores con capacidad para utilizar varios perfiles de Hardware diferentes, como son los portátiles dotados de expansores de buses, se puede tener diferentes configuraciones para los servicios.

ð **Parámetro de inicio**. Normalmente los servicios suelen leer su configuración de inicio desde el registro, aunque se ha provisto un mecanismo para pasar parámetros al servicio al estilo del paso de parámetros en línea de comandos.

GESTIÓN DE SERVICIOS EN NT

El sistema de servicios suele ser el mayor causante de problemas en NT, dado que la mayor parte de los componentes del sistema operativo se hayan implementados como servicios. Entender el funcionamiento del sistema de servicios permite solucionar muchos de los problemas de administración que aparecen en NT. Normalmente la mayoría de los servicios informan de su estado de funcionamiento en el Visor de sucesos, aunque en caso de problemas se deben investigar varios aspectos:

ð Correcta instalación del servicio. Es lo más complicado, ya que aunque muchos servicios son fáciles de instalar y configurar, hay servicios que por no disponer de aplicaciones que cuidan de su instalación y gestión o que no están bien documentados, pueden producir fallos o mal funcionamiento.

ð Configuración de la cuenta de inicio del servicio. Hay muchos servicios que al no ejecutarse con la cuenta del sistema necesitan que se establezca una serie de permisos y privilegios para la cuenta cn la que se inician. Cuando se trabaja en un dominio y se va a utilizar un servicio en varios ordenadores diferentes, conviene utilizar cuentas del comino con los privilegios adecuados. Hay que tener cuidado, ya que muchos administradores tienden a asignar demasiados permisos a las cuentas de servicos.

ð Conviene hacer pruebas con algunos servicios activados y luego desactivarlos. El consejo fundamental es que aquellos servicios que instala por defecto NT no conviene desactivarlos, a menos que se sepa lo que se está haciendo. Por ejemplo desactivar el servicio ISA Plug & Play no permite acceder a la mayoría de los modems instalados.

ð A la hora de instalar nuevos servicios de terceros en NT conviene emplear aquellos que tengan la interfase de control más depurada, ya que a la larga suele ser necesario. Aq uellos servicios que necesitan modificar el registro directamente son propensos a errores de configuración, ya que el editor de registros no realiza comprobaciones cuando se introducen modificaciones en el registro.

Algunos de los servicios que instala NT.

ð *Administrador de conexión de acceso remoto.*

ð *Administrador de marcado automático de acceso remoto.*

ð *Alerta. Permite enviar alertas administrativas.*

ð *Ayuda de Netbios de TCP/*IP. Integra parte de los servicios del protocolo Netbios sobre TCP/IP

ð *Cliente DHCP*. Este servico permite obtener la configuración del protocolo TCP/IP desde un servidor DHCP.

ð *DDE de r*ed. Este servicio y el siguiente componen el sistema que permite el intercambio dinámico de datos en la red (el portafolios de Windows)

ð *DSDM de DDE de r*ed.

ð *Duplicador de directori*os. Este es el servicio de duplicación de directorios, que se utiliza fundamentalmente en el sistema de inicio de sesión en dominios NY.

ð *Estación de traba*jo. Este servicio se encarga de conectarse a los servidores de ficheros e impresoras de la red Microsoft.

ð *EventLog.* Registra los sucesos para que el Visor de Sucesos los pueda visualizar.

ð *Examinador de equip*os. Este servicio es el encargado de encontrar a todos los demás ordenadores dentro de la red Microsoft.

ð *Inicio de sesi*ón. Este servicio permite iniciar sesión en dominios NT.

ð *Localizador de llamadas a procedimientos remotos (RP*C). Forma parte del sistema RPC.

ð *Mensajer*ía. Este servicio permite enviar mensajes en NT, por ejemplo con el comando NET SEND.

ð *Plug and Pl*ay. Uno de los nuevos componentes Plug and Play para NT. En la versión 4.0 de NT todavía no hay soporte completo para Plug and Play en NT.

ð *Proveedor de seguridad NT* LM. Este módulo permite utilizar el sistema de seguridad Lan Manager de NT.

ð *Schedule.* Es el servicio que permite ejecutar las aplicaciones y comandos a ciertas horas. Normalmente se envían comandos a este servicio mediante el comando AT de NT.

ð *Servicio de RPC (llamada a proc. Remot*o). Forma parte del sistema RPC.

ð *Servicio de telefonía.*

ð *Servid*or. Es el servidor de ficheros e impresoras de red.

ð *Servidor de acceso remo*to. Es el responsable de permitir el acceso remoto vía módem al ordenador.

ð *Servidor del portapapel*es. Permite compartir datos entre aplicaciones.

ð *Spool*er. Es la cola de impresión de NT.

ð SAI. Es el servicio de alimentación ininterrumpida.

SISTEMA

Este Panel de Control permite ajustar parámetros generales del sistema.

ð **Gener**al. La pestaña general nos da información sobre el sistema commo puede ser:

− versión del sistema operativo

− El usuario y empresa registrados, con el número de registro.

− Equipo (procesador, arquitectua y memoria RAM instalada)..

ð **Rendimiento.** La pestaña rendimiento permite ajustar dos parámetros importantes: el rendimiento de la aplicación en primer plano y la memoria virtual (ficheros de paginación). El botón Cambiar nos lleva al cuadro de diálogo de Memoria Virtual.

El cuadro de diálogo de Memoria virtual nos permite ajustar los archivos de paginación y de registro. Este cuadro de diálogo permite ver todos los ficheros de intercambia creados. Para cada unidad de disco se puede establecer un fichero de intercambio, que tendrá un tamaño mínimo y máximo. Este cuadro de diálogo nos indica el total de espacio de intercambio disponible para el sistema y las aplicaciones.

También en este cuadro de diálogo se puede establecer el tamaño del registro máximo. Esto evita que el mal funcionamiento de una aplicación pueda desbordar el registro. Normalmente no hace falta modificar el tamaño sugerido por el sistema..

ð **Entrono.** La pestaña entorno fija las variables de entrono tanto para el sistema como para el usuario actual. Los cambios introducidos en este cuadro se hacen permanentes. El comando set de la línea de comandos permite establecer variables de entorno de modo temporal. Algunos

programas necesitan fijar variables de entorno especiales, que se pueden fijar en un fichero .bat antes de lanzar el programa.

ð **Inicio/Apagado.** La pestaña de Inicio y Apagado permite configurar:

− La opción predeterminada para el arranque del sistema. Esta configuración se guarda en el fichero boot.ini, que es un fichero oculto y de sólo lectura que se guarda en el directorio raíz de la partición activa. Este fichero es de texto llano, fácilmente editable.

− Las opciones de recuperación del sistema, es decir, el modo de comportarse el sistema ante un error grave..

El Administrador de usuarios

En NT hay dos tipos de usuarios, aquellos que pertenecen a una máquina que corre NT WK o Server y aquellos que pertenecen a un dominio NT. Para cada uno de estos tipos de usuarios existe una herramienta de administración: el administrador de usuarios incluido en NT Workstation y el administrador de usuarios para dominios incluido en NT Server. El funcionamiento de ambos es muy similar, pero el administrador de usuarios para dominios dispone de más opciones. Por ello, se describirá el administrador de usuarios para dominios.

Las tareas que se pueden realizar con el administrador de usuarios:

− Añadir, modificar y eliminar usuarios del dominio.

− Añadir, modificar y eliminar grupos locales y globales del dominio.

− Fijar el plan de cuentas y contraseñas en el dominio.

− Fijar la política de derechos de usuario en el dominio.

− Establecer el sistema de auditoria en el dominio.

− Establecer relaciones de confianza entre dominios.

CREACIÓN Y MODIFICACIÓN DE USUARIOS EN EL DOMINIO.

Para crear un usuario se pulsa ***Usuarios\Nuevo*** y se completa el cuadro de diálogo..

En este cuadro hay que rellenar una serie de campos:

ð **Nombre de usuario:** Es el identificador que representa al usuario en el dominio. Debe ser una

palabra completa, sin espacios en blanco ni caracteres especiales, de hasta 14 caracteres [verificar]. este identificador debe ser único en el dominio. Se le suele conocer también como nombre de cuenta o login. Este identificador es el que se debe suministrar, junto con la contraseña, para iniciar sesión en un dominio NT.

ð **Nombre completo:** Es el nombre completo del usuario. Si este usuario es una persona se suele escribir el nombre u apellidos.

ð **Descripci**ón. Conviene añadir una descripción de la labor, grupo de personas o departamento al que pertenecen el usuario, sobre todo si la base de datos de usuarios en el dominio es grande.

ð **Contrase**ña. Aquí se debe escribir la contraseña para el usuario. Puede incluir espacios, mayúsculas y minúsculas, e incluso caracteres especiales. NT admite hasta 14 caracteres. Cuando se va escribiendo aparecen asteriscos, y una vez completada en el cuadro aparece una línea de asteriscos, siempre de la misma longitud.

ð **Repetir contraseña.** Hay que introducir de nuevo la contraseña, para comprobar que se ha escrito correctamente.

Tras estos campos aparecen una serie de botones activables:

ð **El usuario debe cambiar su contraseñ**a. La primera vez que inicia sesión en NT se va a solicitar que introduzca una nueva contraseña. Habitualmente los administradores crean los usuarios nuevos con contraseñas del tipo cambiame, que obligan al nuevo usuario a cambiar su contraseña al iniciar sesión por primera vez.

ð **El usuario no puede cambiar su contraseña.** Se utiliza en tareas administrativas especiales, y bloquea el cambio de contraseña por parte del usuario.

ð **La contraseña nunca caduca.** Desactiva la caducidad de contraseñas para esta usuario. Se utiliza normalmente sólo para algunos usuarios que lo necesitan.

ð **Cuenta desactiva**da. Permite bloquear la cuenta fácilmente sin borrarla. Se suele utilizar cuando el usuario no va a iniciar sesión durante un periodo de tiempo o cuando se va a cambiar la configuración o entorno del usuario y se necesita que no pueda acceder temporalmente al sistema..

Al final del cuadro de diálogo aparecen varios botones:

ð **Grupos.** Permite establecer los grupos a los que pertenece un usuario. En NT hay dos tipos de grupos:

ð **Grupos globales.** Válidos para dominios en los que se confían. Aparecen marcados con el icono de grupo global.

ð **Grupos locales.** Son grupos locales al servidor o estación de trabajo.

Además se puede asignar un grupo primario para el usuario [Este grupo es utilizado en entornos Macintosh]

ð **Perfil.** Permite controlar las características del entorno de un usuario.

Se puede establecer:

ð **Perf**il. Nombre del fichero que representa el perfil del usuario para NT. Hay que escribir un fichero en formato UNC (Univer name convention), es deci r:

ð \\servidor\recurso\directorio\fichero.bat.

ð **Archivo de inic**io. Asigna un archivo que se ejecutará al iniciar la sesión de red en el dominio. El archivo debe residir en el servidor que valida el inicio de sesión. Este fichero se debe hallar en la carpeta *NETLOGON* del servidor que valida el inicio de sesión.

ð **Directorio de trabajo.** Admite dos modalidades de uso.

ð **Ruta de acceso local.** Utilizar una ruta local al ordenador en que se inicia la sesión..

ð **Conectar** una letra de unidad a una unidad de red del tipo \\servidor\recurso.

ð A. El directorio de trabajo es el que aparece por defecto en los cuadros de diálogo de guardar un fichero en una aplicación Windows.

ð **Horas.** En el botón Horas podemos acceder al cuadro de diálogo de Horas de inicio de sesión.

En este cuadro de diálogo se pueden fijar las horas de inicio de sesión en los servidores del dominio, en intervalos de 1 hora, para cada día de la semana. En principio una vez iniciada la sesión el usuario puede seguir trabajando en los servidores, aunque se puede modificar esto para que los servidores cierren la sesión del usuario al terminar las horas permitidas, mediante el cuadro de

diálogo Plan de cuentas en el menú de Directivas del Administrador de Usuarios.

ð **Iniciar desde.** Este cuadro de diálogo permite seleccionar los ordenadores desde los cuales un usuario puede iniciar sesión. Se pueden especificar hasta 8 ordenadores que ejecuten NT, o permitir el inicio en todos los ordenadores del dominio.

ð **Cuenta.** El cuadro de diálogo Información de cuenta permite especificar el tipo de cuenta y su duración. Se puede elegir que la cuenta caduque en una fecha determinada o que no tenga caducidad. También se puede especificar si es una cuenta global o local..

ð **Marcado.** El cuadro de diálogo de Marcado permite especificar las propiedades de marcado para el usuario.

MODIFICAR UN USUARIO.

Utilizando el menú ***Usuario\Propiedades*** o haciendo doble clic sobre un usuario o grupo se puede modificar el mismo.

Al modificar un usuario se acceden a los mismos cuadros de diálogo empleados al crearlo salvo que ahora aparece una casilla para cuentas bloqueadas. Si el bloqueo de cuentas está activado en el dominio y el usuario ha fallado el número de veces limitado para ese dominio, esta casilla aparece activada. Al desactivarla, la cuenta del usuario es desbloqueada.

Nota importante: existe una ligera demora al cambiar las propiedades de un usuario o grupo del dominio, debido a que la base de datos de usuarios del dominio tarda unos minutos en actualizarse en los controladores secundarios. Se puede forzar la actualización inmediata mediante la sincronización manual de los servidores.

CREACIÓN DE GRUPOS

Para un NT Workstation (o Server configurado como servidor) el administrador de usuarios permite crear grupos locales, que sólo tienen validez en el propio ordenador. El administrador de usuarios para dominios permite crear dos tipos de grupos: globales y locales. Los grupos locales pueden obtener permisos en los servidores del dominio propio. Pueden ser miembros de los grupos locales los miembros del dominio, los grupos globales del dominio y los grupos globales de otros

dominios en los que se confía. Los grupos globales tienen como miembros a los usuarios del dominio y se pueden utilizar tanto en los servidores del dominio como en las estaciones de trabajo del dominio. También se pueden usar en otros dominios en los que se confía.

CREACIÓN DE UN GRUPO GLOBAL NUEVO.

Para añadir un grupo global nuevo se selecciona el menú ***Usuario\Grupo Global nuevo*** y se proporcionan en el cuadro de diálogo el nombre del grupo y una descripción opcional. Podemos además añadir usuarios al grupo.

CREACIÓN DE UN GRUPO LOCAL NUEVO

Para añadir un grupo local nuevo se selecciona el menú ***Usuario\Grupo Local nuevo*** y se proporcionan en el cuadro de diálogo el nombre del grupo y una descripción opcional. Podemos además añadir usuarios al grupo.

USOS DE GRUPOS LOCALES Y GLOBALES.

Cuando se crea un dominio el programa de instalación de NT crea una serie de grupos globales y locales del dominio. También se crea la cuenta del administrador del dominio, y se añade al grupo administradores del dominio.

El grupo administradores que se ha creado permite administrar todos los servidores del dominio. NT añade al grupo local administradores el grupo administradores del dominio. De igual manera ocurre con el grupo de usuarios e invitados.

Cuando una estación de trabajo es añadida al dominio, NT añade automáticamente los tres grupos globales del dominio (administradores, usuario e invitados del dominio) a los grupos locales correspondientes de la estación de trabajo..

Los grupos locales se utilizan para asignar tareas especiales en las estaciones de trabajo o servidores del dominio. Por ejemplo se pueden crear los grupos especiales para trabajar con el recurso como una impresora láser en color, cuyo acceso queremos restringir. Uno lo podemos llamar Administradores de láser color y otro Usuarios de láser color. Ahora basta dar permisos de impresión al grupo Usuarios de láser color y control total al grupo Administradores de láser

color. Para añadir usuarios a estos grupos bastaría añadir al grupo Administradores de láser color el grupo Administradores del dominio y al grupo Usuarios de láser color los miembros del dominio autorizados a imprimir en ella. Este último paso lo podemos hacer de un medio más eficiente si creamos un grupo global Usuarios de impresora láser color y añadimos este grupo al grupo local Usuarios de láser color. Para dar permisos de impresión a los usuarios y grupos utilizaremos el Administrador de Impresión de dicha impresora, accesible desde el menú de inicio ***Configuración\Impresoras***

Cada usuario en NT debe pertenecer a uno o varios grupos globales o locales, indistintamente. Los grupos locales se definen en cada estación de trabajo NT o en cada servidor. Para los servidores hay dos posibles configuraciones : si el servidor está configurado como controlador de dominio, primario o secundario, los grupos locales son los que se definen para todos los servidores controladores del dominio. Es decir, todos los controladores del dominio comparten la misma lista de grupos locales. Para los servidores configurados como servidor, los grupos locales se definen en el propio servidor, del mismo modo en que se hacen con las estaciones de trabajo.

La siguiente tabla muestra los grupos de que se pueden crear en NT y los usuarios y grupos que les pueden añadir.

Usuarios que se pueden crear en NT Workstation y Server
(no controlador de dominio)

Usuarios y Grupos que se pueden añadir a los grupos.

Grupos Locales

ð Usuarios Locales

ð Usuarios del Dominio

ð Grupos Globales del Dominio

ð Grupos Globales y Usuarios Globales de otros dominios en los que se confía.

Usuarios Locales

Usuarios que se pueden crear en NT Server controlador de dominio

Usuarios y Grupos que se pueden añadir a los grupos.

Grupos Locales

ð Usuarios Locales

ð Usuarios del Dominio

ð Grupos Globales del Dominio

ð Grupos Globales y Usuarios Globales de otros dominios en los que se confía.

Usuarios Locales

Grupos Globales Usuarios del dominio

Usuarios del dominio

ADMINISTRACIÓN DEL PLAN DE SEGURIDAD.

En NT se pueden fijar una serie de directivas comunes para todo el dominio. Entre estas se puede fijar el plan de cuentas para el dominio, que fija propiedades de las cuentas tales como la política de contraseñas, el plan de derechos de usuarios, que permite asignar determinados permisos genéricos a usuarios o grupos del dominio, o el plan de auditoria, que permite activar los elementos del sistema de auditoria en el dominio.

ADMINISTRACIÓN DEL PLAN DE CUENTAS.

Desde el menú ***Directivas\Cuentas*** podemos acceder al cuadro de diálogo Plan de cuentas.

En este cuadro podemos fijar las limitaciones de las contraseñas y el sistema de bloque de cuentas.

Cuando se ha seleccionado caducidad para la contraseña de un usuario, la contraseña utilizará las opciones elegidas en este cuadro de diálogo. Se puede elegir:

ð *Duración máxima de la contrase*ña, en días.

ð *Duración mínima de la contrase*ña, para que el usuario cambie dos veces su contraseña y vuelva a usar la contraseña antigua.

ð *Longitud mínima de la contrase*ña. Las contraseñas con más de 6 caracteres son difíciles de saltar por métodos de asalto masivo (crackers), también llamados de fuerza bruta. Esto es útil en redes conectadas a Internet.

ð *Historia de la contrase*ña, que obliga al usuario a no repetir las últimas contraseñas.

ð *Bloqueo de Cuentas*

El sistema de bloqueo de cuentas permite a los controladores de dominio reaccionar frente a los intentos fallidos de iniciar sesión en el dominio. Si se activa el bloque de cuentas entonces al alcanzarse el numero de intentos especificado la cuenta es bloqueada. Su el número de intentos fallidos no alcanza al especificado, el usuario puede esperar el tiempo fijado en restablecer cuenta para poder volver a intentarlo. Fijando por ejemplo estos parámetros a 4 intentos y 10 minutos suele bastar para disuadir de accesos no autorizados. Una vez bloqueada la cuenta se puede elegir entre desbloqueo automático o manual, con intervención del administrador del dominio.

También en este cuadro de diálogo se puede seleccionar si los usuarios remotos serán desconectados de los servidores al acabar su tiempo de conexión y si un usuario debe iniciar sesión en una estación de trabajo para poder cambiar su contraseña..

ADMINISTRACIÓN DEL PLAN DE DERECHOS DE USUARIOS.

Los derechos de usuarios son una serie de permisos que no se aplican sobre un objeto concreto, como un fichero, impresora o directorio, sino que se aplican al sistema completo. Estos permisos tienen prioridad sobre los permisos asignados sobre los objetos del sistema. Se pueden asignar a cada tipo de derecho de usuario los usuarios o grupos de usuarios a los que se necesite otorgar ese derecho.

Los derechos de usuarios pueden ser modificados desde el cuadro de diálogo Plan de derechos de usuarios accesible desde el menú ***Directivas\Derechos de usuari***os.

Si se activa la casilla *Mostrar derechos de usuario avanzados* se pueden ver algunos derechos de usuarios más específicos. Normalmente los derechos de usuario asignados por NT asignan derechos suficientes a los grupos de usuarios creados por NT. Cuando se instalan algunos servicios, como servidores de correo, de Web y similares suele ser necesario cambiar algunos de estos derechos. Los más frecuentes suelen ser:

ð **Iniciar sesión como servic**io. Permite asignar un usuario a un servicio. Suele ser usuario en

servidores de ficheros tipo FTP, Gopher y Web, ya que permite asignar permisos a los ficheros para ese usuario, limitando el acceso a otros ficheros del sistema. También lo usa el servicio de duplicación de directorios.

ð **Iniciar sesión como proceso por lot**es. Este derecho está pensado para los servicios que atienden las peticiones de usuarios en forma de transacciones, como por ejemplo servidores POP3 y otros. Actualmente no está implementado en el sistema operativo, pero algunos servicios verifican que el usuario posea este derecho antes de atender su petición.

RELACIONES DE CONFIANZA ENTRE DOMINIOS Y MÚLTIPLES DOMINIOS

El sistema de dominios de NT tiene actualmente un grave inconveniente: no existe una jerarquía de dominios. En una red pueden coexistir múltiples dominios, pero todos se hayan al mismo nivel. Cada dominio puede gestionar correctamente varias decenas de ordenadores, incluso centenares, y una gran cantidad de usuarios, en torno a las decenas de miles. Cuando la organización es compleja, por un número de usuarios o equipos elevados y se quiere simplificar la gestión se puede recurrir a un sistema de múltiples dominios.

En un sistema de múltiples dominios, se puede establecer unas relaciones entre ellos de manera que los usuarios, recursos y equipos sean reconocidos en diferentes dominios− Si no se establecen relaciones de confianza entre dos dominios las cuentas de usuario de un dominio no serán válidas en el otro dominio. Establecer relaciones de confianza entre dominios permite que los miembros de un dominio puedan reconocer las cuentas de usuario de otros dominios..

CREACIÓN DE UNA RELACIÓN DE CONFIANZA ENTRE DOS DOMINIOS

Para entender como funcionan las relaciones de confianza vamos a estudiar un ejemplo de utilización. El escenario es el siguiente:

Suponemos una configuración sencilla, con sólo dos dominios, Dominio A y Dominio B. El usuario DominioB\pepe desea imprimir en una impresora del Dominio A, por ejemplo

\\Servidor1\laser.

Si configuramos la impresora para que todos los usuarios puedan imprimir, dando al usuario DominioA\Todos el permiso de impresión, el usuario Dominio B \pepe podrá imprimir, ya que Todos también incluye a los usuarios de otros dominios. Lo que necesitamos es un modo para asignarle explícitamente al usuario Dominio B \pepe el permiso de impresión sin utilizar el usuario Todos. Si intentamos añadir el usuario DominioB\pepe, veremos que las herramientas administrativas no lo permiten, ya que sóo permiten añadir usuarios de DominioA.

¿Qué ocurre cuando el usuario DominioB \pepe intenta imprimir? Si el usuario DominioA\Todos no tiene permiso de impresión, el servidor de impresión intentará validar al usuario DominioB\pepe. Al pertenecer a un dominio diferente el servidor de impresión no pude validar al usuario, por lo que no le permitirá imprimir. Ya que la cuenta DominioB \pepe no pertenece al dominio, debemos configurar los dominios DominioA y DominioB de modo que permitan que el servidor d impresión de A pueda autentificar mediante los controladores de dominio de DominioB al usuario de su dominio pepe. El método que utiliza NT para delegar la autentificación es la relación de confianza entre dominios. La relación de confianza entre dos dominios permite a los servidores de un dominio consultar la base de datos de usuarios y equipos de otro dominio para autentificar a un usuario de ese dominio. Realmente el proceso exacto que desarrolla la consulta no es interesante desde el punto de vista de la administración. Lo importante es que para poder autentificar al usuario de DominioB en DominioA, DominioA debe poder consultar la base de datos de usuarios de DominioB.

Las relaciones de confianza son unidireccionales, es decir, puede existir una relación de confianza de A a B y otra de B a A. Por tanto, cuando se crea una relación de confianza entre dominios, se debe decidir qué dominios deben permitir consultar su base de datos.

Veamos todo con el ejemplo propuesto. Ya que DominioB \pepe debe imprimir en el servidor de impresión de DominioA, la base de datos de usuarios de DominioB debe ser accesible para los miembros del DominioA. Por ello debemos configurar los dos dominios:

ð DominioB. Abrimos el Administrador de usuarios para Dominios y seleccionamos el menú ***Directivas\Relaciones de confianza***. Aparece un cuadro de diálogo con las relaciones de confianza establecidas actualmente..

Ahora pulsamos el botón ***Agregar*** de la sección ***Dominios de confianza***. Aparece el cuadro de diálogo ***Agregar dominio que confía***.

Escribimos el nombre de dominio que va a consultar nuestra base de datos, es decir DominioA, y una contraseña para que pueda consultar la base de datos de usuarios.

ð DominioA. Abrimos el Administrador de usuarios para dominios y seleccionamos ***Directivas\Relaciones de confianza***. En el cuadro de diálogo de ***Relaciones de confianz***a. Pulsamos el botón ***Agregar*** de la sección ***Dominios en los que se confía***.

Aparece el cuadro de diálogo ***Agregar dominio en el que confiar***.

Introducimos el DominioB y la contraseña que se ha creado en el DominioB. Si todo funciona correctamente un mensaje en pantalla nos informará de que la relación de confianza se ha establecido.

Si necesitamos establecer la relación de confianza inversa deberemos repetir los mismos pasos intercambiando los papeles de cada dominio.

Nota: es muy difícil recordar quién el dominio que confía, cuál es el que debe confiar y el resto de la terminología empleada en estos cuadros de diálogo. El truco para acertar a la primera es el siguiente: nos fijamos en quién permite consultar su base de datos de usuarios. Este dominio es el que debe fijar la contraseña, luego en su cuadro de diálogo de *Agregar* debe aparecer *contraseña* y *repetir contrase*ña. El dominio que debe consultar la base de datos de usuarios debe proporcionar dicha contraseña, luego en el cuadro de diálogo *Agregar* sólo aparece *dominio* y *contrase*ña.

Recordando el truco de los cuadros agregar y quién es el que debe compartir su base de datos de usuarios, es muy fácil establecer la relaciones de confianza.

CONFIGURACIONES PARA MÚLTIPLES DOMINIOS

Mediante las relaciones de confianza se pueden establecer configuraciones para múltiples dominios:

ð *Configuración con un solo maest*ro. En esta configuración un dominio hace las veces de dominio maestro y los demás dominio son los dominios subordinados.

En esta configuración los dominios subordinados pueden consultar la base de datos de usuarios del maestro, pero no al revés, es decir , las cuentas de usuarios y grupos globales del dominio maestro son válidas en los dominio subordinados, pero no al revés.

Esta configuración es la habitual en una organización en la que un dominio se encarga de administrar los demás, pero cada uno de los dominios está aislado de los demás. E dominio maestro pudría ser la sede central y los subordinados cada una de las delegaciones. Bastaría incluir en el grupo de administradores local el grupo de administradores global del dominio maestro en el grupo administradores local de cada uno de los dominios subordinados, para que los administradores del dominio maestro pudiesen administrar los equipos y usuarios de los dominios subordinados.

ð Configuración múltiples maestros.

En esta configuración se establecen ambas relaciones de confianza entre todos los dominios.

De esta manera las cuentas de cada dominio serían válidas en los demás. Esta organización se establece cuando no hay un dominio con un papel de maestro o administrador.

ð *Configuraciones mixt*as. Se puede establecer cualquier mezcla de estos tipos de relaciones de confianza, para adaptarse a la estructura de la organización.

USO DE LOS GRUPOS GLOBALES Y LOCALES CON RELACIONES DE CONFIANZA

Cuando se establece una relación de confianza entre dominios no se modifica ninguna directiva del dominio ni la base de datos de los dominios. Para que los usuarios de los dominio puedan realizar acciones en el otro dominio, se les deben permitir explícitamente. Por ejemplo:

ð Para añadir los administradores del dominio B a los de A, hay que establecer la relación de confianza de B a A y luego añadir al grupo administradores de los controladores de dominio A el grupo de administradores del dominio B.

ð Para que el usuario DominioB\pepe pueda imprimir en un equipo miembro de A hay que añadirle a los usuarios permitidos en el servidor de impresión del DominioA

ð Para que los usuarios de DominioB puedan iniciar sesión en un equipo de A hay que añadirle al grupo de usuarios del equipo..

FUNCIONAMIENTO DEL MONITOR DEL SISTEMA.

Cada uno de los objetos del sistema operativo contiene una serie de contadores que permiten conocer el estado de actividad del objeto. Para algunos de estos objetos, los contadores deben ser activados antes de ejecutar el monitor del sistema. Ejemplos de objetos que podemos monitorizar son las unidades de disco físicas, los procesadores, la memoria física, la memoria caché, y otros componentes, que incluyen los componentes del sistema de red. Incluso algunas aplicaciones como servidores SQL y otros pueden añadir sus propios tipos de objetos y contadores..

GRÁFICOS.

El primer método para visualizar los contadores para un objeto es el gráfico. En un gráfico se representa cada uno de los contadores como líneas de colores o barras de histograma.

Con el menú ***Edición/Añadir al gráfico*** se pueden añadir líneas o barras al gráfico, que representen nuevos contadores.

Al seleccionar este menú aparece el cuadro de diálogo ***Añadir al gráfico.***

En primer lugar se debe elegir el ordenador que se va a monitorizar. Esto permite visualizar varios contadores procedentes de diferentes ordenadores.

Luego se debe elegir el tipo de objeto. Los tipos por defecto suelen ser: Archivos de paginación, caché, disco físico, disco lógico, examinador, memoria, objetos, procesador, procesos, redirectorios, servidor, sistema e hilos (threads).

Algunos de estos objetos poseen más de una instancia. Por ejemplo en disco físico y lógico podremos tener varios discos y en cada disco varias particiones. Para el caso de procesos e hilos las instancias que aparecen dependen de qué aplicaciones se estén ejecutando en el sistema..

Para cada uno de los objetos podemos seleccionar cualquiera de los contadores que posee.

Luego se debe elegir la apariencia del contador en el gráfico (color, escala, ancho y estilo) aunque el monitor del sistema elige valores por defecto. Además existe la opción explicar, que nos da una

breve descripción del significado del contador.

Dentro del menú ***Opciones/Gráfico*** accede al cuadro del diálogo ***Opciones del gráfi***co:

En este cuadro se puede elegir si se necesita leyenda, barra de valores, rejillas horizontal y vertical, o etiquetas vertida.

Se puede elegir además el tipo de gráfico: de líneas o histograma (barras verticales). El gráfico posee dos modos de actualización automática, con posibilidad de elegir el intervalo de actualización en fracciones de segundo, o manual, cada vez que se elige el menú ***Opciones/Actualizar ahor***a.

ALERTAS.

Las alertas permiten monitorizar contadores específicos de manera que se produzca una alerta al sobrepasarse por exceso o defecto un cierto valor asignado a un contador. Esto permite incluso ejecutar una aplicación al producirse la alerta. Para añadir una nueva alerta se selecciona el menú ***Edición/Agregar alerta*** que muestra el cuadro de diálogo ***Agregar a alert***a.

Primero se debe elegir el ordenador, al igual que se hizo para el gráfico. Después se debe elegir el objeto, el contador y la instancia de un modo análogo a como se hace para el gráfico.

Luego se puede elegir el color identificativo de la alerta. A continuación se elige el valor que desencadena la alerta. Se debe introducir un valor en la opción ***Alertar*** si y luego se selecciona si el límite es superior o inferior..

Además tenemos la opción para ejecutar un programa la primera vez que se produzca la alerta o cada vez que se produzca.

En el menú ***Opciones/Alerta*** se puede abrir el cuadro de diálogo ***opciones de alerta***.

Se puede elegir que se cambie automáticamente a la pantalla de alerta; que se añada la alerta al registro de aplicaciones del sistema, o que se envíe un mensaje de red al nombre de red especificado.

Al igual que para el gráfico, se puede elegir el tipo de actualización, manual o automática.

REGISTRO.

El registro permite recoger la información de los diferentes contadores seleccionados volcándolos

sobre un archivo de registro (.log). Se pueden añadir objetos al registro mediante el menú ***Edición/Agregar al regist***ro, que muestra el cuadro de diálogo ***Agregar al regist***ro

En este cuadro se puede elegir el ordenador a monitorizar y el objeto. Desde el menú ***Opciones/Registro*** podemos acceder al cuadro de diálogo ***Opciones del regist***ro:.

El registro se va a guardar como un archivo *.log. En este cuadro de diálogo podemos modificar el intervalo de tiempo en que se van a añadir datos al archivo registro, así como elegir actualización manual. El botón ***Iniciar registro/detener registro*** da comienzo y para el registro de la actividad del sistema.

ATRIBUTOS EN NTFS

El sistema de particiones NTFS define muchos tipos de atributos estándar dentro de os ficheros y directorios, como por ejemplo:

ð Información estándar. Almacena fechas, enlaces, y otros.

ð Nombres de ficheros. Almacena nombres de los ficheros en formatos cortos, largos y enlaces duros POSIX.

ð Lista de atributos. Incluye información para acceder a los registros extendidos de atributos en ficheros largos.

ð Lista de control de acceso

ð Datos. Contiene los datos binarios del fichero.

ð Raíz y Localización de los índices. Empleados para registros de tipo directorio.

ð Volumen. Incluye la información del volumen.

ð Mapas de bits. Indica los ficheros que están siendo usados por los ficheros o la MFT.

ð Atributos extendidos. Usados en OS/2

ð Flujos (streams). NTFS permite que un fichero contenga un atributo de datos principal y datos adicionales almacenados como flujos separados. Cada flujo permite almacenar datos separados, y se puede acceder a cada flujo añadiendo el nombre del flujo del fichero al nombre del fichero, separado por el signo :, como por ejemplo: Mifichero.dat:flujo1.

ð Compresión y tipo de compresión. Permite indicar si un directorio o fichero ha sido comprimido. El sistema de compresión de NTFS trabaja de forma transparente a nivel de atributos en los ficheros, por lo que es muy fiable y extensible.

LOS FICHEROS DE SISTEMA NTFS

La partición NTFS incluye una serie de ficheros del sistema:

ð $MFT. Contiene la Tabla de Ficheros Maestra

ð $MtfMirr. Es la MFT espejo.

ð $LogFile. Es el fichero de transacciones hacia el volumen NTFS. Todos los cambios que se producen en NTFS se registran como una transacción. NTFS no garantiza la integridad de los datos de usuario, sino la integridad y consistencia de la estructura del volumen. ð $Volume. Incluye la descripción del volumen.

ð $AttrDef. Define los atributos en uso en el volumen.

ð $. Representa el directorio raíz del volumen.

ð $Bitmap. Representa un mapa de bits de ocupación del volumen.

ð $Boot. Incluye los sectores de arranque del sistema.

ð $BadClus. Define una tabla de cluster erroneos.

Cuando se crea un volumen NTFS, se reserva espacio para la información del volumen y se decide el tamaño de los clusters NTFS. Se puede optar por cluster entre 512 bytes y 4K bytes. El tamaño de los registros de la MFT se asigna a 1, 2 o 4 Kilobytes, dependiendo del tamaño del volumen.

CREANDO PARTICIONES CON EL ADMINISTRADOR DE DISCOS

Si se dispone de espacio libre en el disco con el administrador de discos se pueden crear nuevas particiones. Para ello se selecciona el espacio libre del disco y se procede a crear una partición. En el menú ***partición\crear*** podemos crear fácilmente una partición normal o extendida. Si el disco deber ser compatible con MSDOS, solo puede haber una partición primario formateada como FAT. Si se ha creado una partición extendida se deben crear unidades lógicas en ella antes de proceder a formatearlas. Para ello se debe primero guardar los cambios realizados con la opción del

menú ***particion\registrar los cambios aho***ra. Una vez que se han creado las particiones y las unidades lógicas podemos formatear la unidad lógica con cualquiera de los dos tipos de formatos, FAT y NTFS. El tipo de formato elegido depende del uso que se vaya a dar a la partición. El formato FAT es más eficiente con particiones pequeñas, de menos de 200 megas,. pero carece de todas las opciones y características avanzadas de la partición NTFS. Por encima de los 200 megas la partición muestra sus limitaciones, por lo que para estos tamaños el rendimiento de esta partición no es idóneo.

Cuando se han cambiado la configuración del sistema conviene además actualizar la información del disco de reparación. Esto se puede realizar mediante la utilidad RDISK, que se puede ejecutar desde la línea de comandos.

ELIGIENDO PARTICIONES PARA UN SISTEMA NUEVO.

Cuando se va a instalar un sistema nuevo, especialmente en el caso de los servidores, conviene planificar el espacio en disco requerido y el formato a aplicar a los discos. Normalmente en el sistema vamos a disponer de un disco de gran capacidad, ya que el sistema operativo por si solo necesita un espacio de unos 100 megas, mas el espacio dedicado a los archivos de paginación, que suelen ser de unos 30−70 megas como mínimo, si se van a tener un número grande de aplicaciones abiertas simultáneamente.

Para el sistema operativo en el caso de un servidor pequeño conviene preparar una partición no muy grande. Normalmente bastará con una partición de 200−300 megas. Esta partición puede ser formateada como FAT, que permite utilizar herramientas de reparación DOS sobre esta partición. El resto del espacio en disco se puede particionar como NTFS, de manera que podamos incluir características avanzadas, como son la compresión de ficheros y directorios, o las características de seguridad y auditoria.

Si el servidor va a ser de tamaño medio, la partición del sistema debería hacerse de un tamaño mínimo de dos gigas. En este caso se puede hacer FAT o NTFS. Si se va a utilizar mirror del sistema se tiene que usar obligatoriamente NTFS.

Si el servidor va a ser un servidor departamental, tomar las siguientes precauciones:

ð Los RAID se harán por hardware, con controladoras RAID avanzadas (tipo Mylex, o soluciones de fabricantes como IBM, HP o Compaq).

ð Se usarán discos SCSI de altas prestaciones (10000 rpm, ultrawide, con intercambio en caliente)

ð La partición de sistema se hará de 4 gigas, en NTFS con espejo.

ð Se procurará utilizar discos de reserva (Hot Spare)

ð Se harán frecuentes discos de reparación con RDISK /S.

Nota: porqué utilizar FAT y no NTFS para el sistema. La mayor parte de las operaciones de lectura y escritura del sistema en los archivos de sistema se realizan utilizando la cuenta del sistema, que tiene total acceso a estos archivos. En principio sólo los administradores y el sistema deberían poder acceder a estos archivos. NT gestiona correctamente estos accesos tanto en NTFS, mediante la seguridad de archivos, como en FAT, que tiene definida una seguridad por defecto para estos archivos. Sin embargo el método de acceso FAT para estos archivos es más rápido, por lo que no es necesario que sea una partición NTFS. Probablemente FAT32 mejorará las prestaciones del acceso a los archivos del sistema FAT, por lo que será la opción recomendada en NT 5.0 para una partición separada de sistema.

Nota: El programa de instalación de NT tiene un bug, que aveces no deja crear particiones de 4 Gigas sobre discos SCSI, sobre todo en controladoras RAID. El truco consiste en arrancar con un disco de MSDOS, crear una partición de 2 gigas y luego instalar NT como siempre, borrando esta partición. Ahora dejará hacer una partición de 4 gigas (menos de 4096 megas).

Hay que tener en cuenta que si hacemos solo una partición para el sistema, en la que ponemos sistema y datos, podemos correr el riesgo de luego necesitar ampliar la parte de datos de la partición. Al ser una sola partici ón, y contener el sistema operativo, no vamos a poder ampliarla utilizando conjuntos de volúmenes.

AMPLIANDO LOS VOLÚMENES: CONJUNTOS DE VOLÚMENES

El sistema de particiones permite aumentar una partición ya creada sin perder los datos que

contenía dicha partición. Para ello debemos disponer de espacio libre en un disco, que no tiene porqué ser el que contiene la partición a ampliar. Esta partición debe tener formato NTFS y no deber ser la partición que contiene al sistema operativo. Si se han seguido las recomendaciones dadas en el apartado anterior esto no es un problema.

CREACIÓN DE UN CONJU NTO DE VOLÚMENES

Para ampliar una partición se selecciona dicha partición y pulsando la tecla ***Contr***ol se selecciona un espacio libre del disco. Después se selecciona el menú ***partición\ampliar*** conjunto de volúmenes. Esto va a permitir ampliar de una manera rápida y sencilla una partición creada previamente en un disco sin más que añadir un disco adicional al sistema. También se puede crear directamente un conjunto de volúmenes seleccionando varios espacios libres de varios discos, manteniendo siempre pulsada la tecla ***Contr***ol y luego usando el menú ***\partición\crear*** conjunto de volúmenes. Por ejemplo:.

Tras haber elegido la partición que queremos ampliar y el espacio disponible, al pulsar el botón derecho aparece un menú que nos permite ampliar el conjunto de volúmenes. El siguiente cuadro de diálogo nos permite elegir el tamaño del conjunto de volúmenes, que estará formado por los volúmenes ya disponibles más el que se va a crear.

Como siempre, tras haber efectuado cambios en el administrador de discos, debemos registrar los cambios para que tengan efecto, por ejemplo, pulsando el botón derecho sobre el nuevo conjunto de volúmenes.

El conjunto de volúmenes aparece en el administrador de archivos identificado como una única unidad, en color amarillo. Por último, el sistema nos pedirá que reiniciemos para que la partición esté disponible..

OPTIMIZANDO EL ACCESO A LOS VOLÚMENES: LAS BANDAS.

Cuando se crea un conjunto de volúmenes, la organización lógica de los datos es la siguiente: la información se guarda consecutivamente en cada volumen del conjunto. Cuando se llega al tope de uno de los volúmenes, se continúa en el siguiente volumen del conjunto.

Al acceder el sistema a un cilindro cualquiera del disco, las cabezas del disco deben primero posicionarse sobre el cilindro. Esta operación penaliza el acceso al cilindro con una pequeña demora. El sistema de particiones NTFS dispone de un mecanismo que permite reducir este inconveniente: las bandas. Un conjunto de bandas está formado por dos o más volúmenes NTFS, en los que la información va a ser diferente a la empleada en los conjuntos de volumen. En las bandas la información se almacena consecutivamente en cilindros de diferentes discos.

Normalmente las ordenes enviadas a los discos para posicionarse en los cilindros correspondientes pueden ser procesadas simultáneamente por todos los discos. Esto repercute en un ahorro de tiempo, ya que el tiempo típico que suel e emplear una unidad de disco habitual en posicionar las cabezas sobre un cilindro es de unos 10 milisegundos.

CREACIÓN DE UN CONJUNTO DE BANDAS

Para crear un conjunto de bandas se procede de modo parecido a como se hizo para el conjunto de volúmenes: se selecciona en dos o más discos diferentes varios espacios libres y se pulsa el menú ***Partición\Crear conjunto de band***as, o se usa el botón derecho del ratón..

El administrador de discos creará particiones del mismo tamaño, que será el tamaño disponible en el disco que menos espacio disponible tenga, por lo que en los demás discos se dejará todavía espacio disponible. Por ejemplo, si un disco tiene 500 megabytes libres y el otro 90, se crearán particiones de 90 megabytes en cada disco para crear las bandas.

Se puede incluso seleccionar un tamaño menor, para dejar espacios disponibles en los discos, quizás para añadir otras particiones.

Como siempre, tras haber creado las bandas, que ahora se muestran en verde en el administrador de discos, debemos registrar los cambios.

Luego hay que proceder a formatear las bandas con formato NTFS, eligiendo opciones como la activación de la compresión de la unidad..

Por último, el administrador de discos nos mostrará la banda preparada para su uso. La banda aparecer á como una sola unidad, de color verde, en el administrador de discos.

TOLERANCIA A FALLOS EN LOS DISCOS: BANDAS CON PARIDAD Y ESPEJOS.

El sistema de particiones NTFS es un sistema bastante tolerante a fallos, ya que la escritura de información en los discos físicos se produce a través de un proceso basado en transacciones. De esta manera el disco habitualmente está protegido frente a caídas del sistema. Sin embargo el sistema de gestión de discos de NT permite añadir mayores características de tolerancia a fallos en las particiones. Esto se logra a través de los **conjuntos de bandas con paridad** y los **discos espe**jo.

Estas funciones sólo están disponibles en la versión NT Server.

Un conjunto de bandas con paridad se comporta de forma parecida a como lo hace un conjunto de bandas normal, salvo que uno de los volúmenes del conjunto de bandas se reserva para guardar información de paridad. Por ello para crear un conjunto de bandas con paridad se necesitan tres o más espacios libres en diferentes discos. Para crear el conjunto de bandas con paridad de seleccionan los espacios libres con el ratón presionando la tecla ***Contr***ol y luego se selecciona el menú ***Tolerancia a fallos\Crear bandas con parid***ad. El procedimiento es análogo a como se crean bandas y conjuntos de volúmenes.

CREACIÓN DE UN ESPEJO

El otro modo de crear un sistema de discos tolerante a fallos en NT es mediante la creación de discos espejo. Un sistema de discos espejo está formado por dos discos en los que se van a crear una partición en cada uno de ellos. La información guardada en ambos discos es la misma. Dicho información se guarda simultáneamente en ambos discos, de manera que si se produce un fallo en uno de los discos, el sistema continúa trabajando con el otro disco. Para crear un sistema de discos espejos debemos seleccionar la partición cuya información queremos duplicar y luego presionando ***Control*** seleccionar un espacio libre en otro disco de tamaño igual o mayor al de la partición a duplicar. Después se selecciona el menú ***Tolerancia a fallos\establecer espejo***.

El administrador de discos creará la partición correspondiente y la unirá a la primera para formar el espejo.

Una vez que ha sido creado el espejo se deben registrar los cambios y guardar la nueva configuración de los discos, tal y como sugiere el administrador de discos. Por último hay que reiniciar el sistema, ya que el sistema debe comenzar a generar el espejo. Si la partición está vacía, el proceso es muy rápido, pero si contiene datos el sistema deberá copiar primero los datos.

Se puede crear un espejo sobre la partición del sistema, siempre que sea una partición NTFS, esto permite evitar utilizar unidades de Backup, más cara y lentas que u disco rápido, sobre todo si se utiliza la configuración más rápida posible: dos controladoras SCSI separadas con un disco en cada una de ellas..

ROMPER DISCOS ESPEJO

Se puede romper el sistema de espejos mediante el menú ***Tolerancia a fallos\Romper el espejo***.

El administrador de discos asignará a cada partición una letra diferente. De esta manera podremos eliminar la partición que no nos convenga, o sustituir uno de los discos por otro.

RECUPERACIÓN DE LOS DATOS

Tras producirse un fallo en un conjunto de bandas o en discos espejos el administrador de discos permite regenerar la información no dañada. Este tipo de situaciones se da en caso de avería grave en el sistema de discos (caída de tensión, aterrizaje de las cabezas sobre la superficie de los discos, etc.) Ante un fallo de este tipo, el sistema de ficheros marca la partición dañada como huérfana. El sistema deja de usar esa partición, utilizando las restantes.

Si el fallo se produce sobre uno de los discos del espejo primero se debe romper el espejo.

Luego se selecciona un espacio libre del tamaño adecuado y se vuelve a generar el espejo. Al reiniciar el sistema los datos se copiaran al disco nuevo automáticamente.

Si el fallo se produce sobre un sistema de bandas con paridad, se debe solucionar un espacio libre del tamaño de las demás bandas y usar el menú ***Tolerancia a fallos\Regenerar***. Cuando se reinicie el sistema, el controlador de tolerancia a fallos del sistema de discos regenerará automáticamente el conjunto de bandas con paridad.

EL ADMINISTRADOR DE IMPRESIÓN.

El administrador de impresión centraliza las tareas efectuadas por el icono impresoras del panel de control de Windows y por el administrador de impresión de Windows, aunque se accede a él desde los mismos lugares que en Windows.

Desde el administrador de impresión se puede crear impresoras, modificar sus propiedades y seguridad, conectarse a impresoras de red y compartir la impresora. Para crear una impresora se selecciona el menú ***Impresora\Crear−impresora***. Aparece el asistente para añadir una nueva impresora.

Cuando se comparte una impresora el administrador puede designar qué usuarios pueden acceder a la impresora desde la red y con qué privilegios.

EL ADMINISTRADOR DE ARCHIVOS.

El administrador de archivos de NT trabaja de modo análogo a como lo hace el de Windows, pero está preparado para asignar seguridad a archivos, directorios y unidades de red.

En NT toda la información de seguridad de los archivos se guarda en el interior de estos.

Esto significa que por una parte no existe una tabla de permisos de los diferentes archivos del sistema, que es el método empleado por algunos sistemas operativos, y por otro que cuando se hacen copias de seguridad, los permisos, al igual que el resto de los atributos de los archivos, se guarda y restaura junto con los datos del archivo. Para establecer los permisos de un archivo basta seleccionar el archivo en el administrador de archivos y seleccionar Seguridad/Permisos.

PERMISOS DE UN ARCHIVO

El cuadro de diálogo que aparece nos muestra la información de seguridad del archivo:.

En el cuadro de diálogo aparecen dos elementos importantes:

ð El propietario del archivo. En NT el propietario de un objeto siempre puede cambiar la información de seguridad del objeto. Adicionalmente en NT los administradores también lo pueden hacer, haciéndose propietarios de él mediante el mecanismo de este archivo. En NT cada archivo, como en general cada objeto, pone una lista con todos los usuarios y grupos que tienen acceso a él,

indicando para cada uno de ellos el tipo de acceso permitido.

ð La lista de usuarios y grupos que tienen acceso al archivo, indicándose el tipo de acceso para cada uno de ellos.

Para añadir nuevos usuarios y grupos a la lista, con sus correspondientes permisos, se pulsa el botón Agregar. Aparece un nuevo cuadro de diálogo:

En este cuadro aparece una lista con todos los grupos de usuarios que se pueden añadir. Si demás queremos enseñar los usuarios del dominio se pulsa el botón ***mostrar usuarios***.

ð En la parte central aparece una lista con los usuarios o grupo que se van añadiendo. Para añadir un usuario o grupo se hace doble clic sobre él.

ð En la parte inferior del cuadro aparece el tipo de acceso que se va a seleccionar para el grupo de usuarios que se está añadiendo. Este tipo es el mismo para todos los que hemos seleccionado. Una vez completada la lista se pulsa aceptar..

ð Si tenemos que añadir permisos para varios usuarios o grupos, pero que van a necesitar diferentes tipos de acceso podemos repetir el proceso anterior el número de veces necesario. Los diferentes tipos de acceso a los archivos son:

Permisos predefinidos Explicación

Lectura (LX) Pueden leer y ejecutar el archivo

Cambio (LWXD) Tiene los permisos de lectura, más los de escritura y

borrado.

Control total Tiene acceso completo a las propiedades del archivo.

Sin acceso No tienen ningún tipo de acceso al fichero.

Acceso especial Se especifican cada uno de los accesos por separado.

El cuadro de diálogo Acceso especial permite modificar cada uno de los tipos de acceso por separado:

Se puede asignar los siguientes tipos de acceso:

Tipo de permiso Explicación

Lectura (R). El usuario puede leer el fichero.

Ejecución (X) El usuario puede ejecutar el archivo, en caso de que este sea ejecutable (en general .exe, .com, .bat o .cmd).

Escritura (W) El usuario puede escribir sobre el fichero

Eliminación (D) El usuario puede borrar el fichero.

Cambio de permisos (P) El usuario puede cambiar los permisos del fichero

Toma de posesión (T El usuario puede tomar posesión del fichero

Sin acceso El usuario no tiene acceso al fichero.

Para saber si un usuario tiene acceso sobre un fichero se puede seguir las siguientes reglas:

ð Se mira si en la lista de permisos aparece el nombre del usuario o alguno de los grupos a los que pertenezca con el tipo de acceso Sin acceso. En este caso el usuario no tiene acceso, aunque se cumpla la siguiente regla..

ð Se mira cada uno de los grupos a que pertenece, además de su nombre. Por cada grupo al que pertenezca se añadirá al acceso permitido el acceso concedido a ese grupo, de manera que el acceso total será la suma de todos los accesos.

PERMISOS EN DIRECTORIOS.

Los permisos en los directorios se gestionan de una forma muy parecida a como se hace para los archivos.

Para los directorios también existe una lista de usuarios y permisos, pero ahora para cada usuario o grupo debemos especificar dos tipos de acceso:

ð **Acceso al director**io. Cada archivo y subdirectorio dentro de un directorio se representa por una entrada o elemento del directorio. El acceso a directorio determina el acceso por parte del usuario a dichas entradas.

ð **Acceso a los ficheros.** Cuando un usuario crea ficheros [y subdirectorios] en el directorio, el acceso a dichos ficheros queda determinado por el acceso a ficheros especificado en el directorio. Se puede dar el caso, estableciendo convenientemente los permisos, de que un usuario cree un

fichero en un directorio y luego no tenga acceso a él.

Los accesos a fichero son los mismos que aparecen cuando se selecciona un fichero. Para los accesos a directorio disponemos de los siguientes:

Tipo de Acceso al directorio Significado

Listado (RX)(Sin

especificar)

Permite obtener un listado del directorio y cambiar a los subdirectorios, pero no asigna permisos a los ficheros.

Lectura (RX) (RX) Permite obtener un listado del directorio y cambiar a los subdirectorios, así como leer y ejecutar los ficheros.

Adición (WX) (Sin especificar)

Permite añadir ficheros y directorios, pero luego no se puede acceder a ellos.

Adición y lectura (RWX)(RX)

Permite añadir ficheros y directorios, así como la lectura y ejecución de los ficheros.

Cambio (RWXD) (REXD) Permite lectura y escritura sobre el directorio y los ficheros que contiene. No permite el cambio de permisos ni la toma de posesión.

Control total Permite todo tipo de acceso sobre los ficheros y directorio.

Acceso especial a directorios...

Permite asignar permisos a las entradas del directorio.

Acceso especial a archivos... Permite asignar permisos a los ficheros del directorio.

También se puede seleccionar los accesos a ficheros y directorios manualmente, como se hacía para los ficheros. Para los directorios se dispone de los siguientes permisos:

Tipo de permiso Significado

Lectura (R) El usuario puede leer, es decir, listar las entradas del directorio.

Escritura (W) El usuario puede añadir ficheros y subdirectorios al directorio

Ejecución (X) El usuario puede cambiar a los subdirectorios del directorio

Eliminación (D) El usuario puede borrar ficheros y subdirectorios del directorio

Cambio de permisos (P) El usuario puede cambiar los permisos de los ficheros y directorios.

Toma de posesión (O) El usuario puede hacerse propietario de los fichero y subdirectorios (tomar posesión de ellos)

TOMA DE POSESIÓN.

El sistema de seguridad de NT asigna un propietario a todos los objetos del sistema. El propietario de un objeto puede cambiar los permisos de un objeto. Las herramientas administrativas de NT permiten tomar posesión de los objetos, por ejemplo ficheros, directorios, impresoras, unidades de red, etc. Cuando un usuario toma posesión de un objeto pasa a ser el propietario de dicho objeto. Las herramientas administrativas de NT no permiten ceder la posesión de un objeto.

El uso fundamental de la toma de posesión es crear directorios personales. Un administrador puede crear un directorio para un grupo de usuarios y asignarle control total para esos usuarios. Un usuario miembro de ese grupo podría crearse un directorio personal.

Para ello crearía un directorio y luego se asignaría así mismo control total sobre él. Después de tener control total bastaría con que tomase posesión de ese directorio para que el resto de los usuarios de su grupo no pudieran acceder a él.

En NT los administradores siempre pueden tomar posesión de un objeto, de manera que siempre tienen un modo de acceso a los recursos de los usuarios. Este mecanismo deja un rastro fácilmente observable por los usuarios, ya que una vez que los administradores han tomado posesión de un recurso no pueden dejar de ser propietarios del recurso.

Para tomar posesión de un archivo o directorio se selecciona en el administrador de archivos y se usa ***Seguridad/Propietario*** y se pulsa toma de posesión..

Inicio de sesión en Dominios

Cuando un usuario inicia sesión en un dominio se puede configurar su entorno utilizando dos mecanismos basados en el dominio:

ð *Ejecución de un archivo de inic*io. Cuando un usuario inicia sesión en un dominio, el servidor que

valida el inicio de sesión al usuario comprueba si al usuario se le ha asignado un archivo de inicio de sesión, también llamado logon script. Este archivo se ejecuta en el propio cliente, no en el servidor, por lo que el archivo de inicio de sesión debe estar preparado para ser ejecutado en los sistemas en los que el usuario puede iniciar sesión.

ð *Configuración del perfil del usuar*io. Los perfiles de usuario fueron introducidos con Windows NT y sirven para configurar el entorno de trabajo para el usuario. Actualmente existen dos tipos de perfiles de usuario: los que se utilizan en NT y los que se utilizan en Windows 95.

EL ARCHIVO DE INICIO DE SESIÓN.

Este archivo puede ser: un ejecutable dos, un ejecutable Windows o un archivo de proceso por lotes. Normalmente el tipo de archivos más usado va a ser el archivo de procesos por lotes. Este archivo es procesado en el cliente. Aquí aparece un problema, y es que este archivo posee las limitaciones del sistema en el que se ejecuta el archivo. Una de las limitaciones más importantes aparece en las máquinas que ejecutan Windows 3.x , ya que los archivos de procesos por lotes de Windows 3.x no son capaces de ejecutar aplicaciones Windows. En NT y Windows 95 existe el comando start, capaz de lanzar aplicaciones Windows desde la línea de comandos de una ventana MSDOS desde el archivo de inicio de sesión.

El archivo de proceso por lotes se suele utilizar para obligar a ejecutar algún programa al usuario cada vez que inicie sesión. Un ejemplo típico son los programas lectores de correo. Si un usuario tiene su programa de correo en un directorio de un servidor de correo, un ejemplo de archivo de inicio podría ser:

En este ejemplo suponemos que el programa se puede lanzar desde el ordenador donde el usuario inicia sesión. Esto es si mail.exe es un programa para Windows el sistema debe ser capaz de arrancarlo. Con NT y Windows 95 no hay problema. En Windows 3.x probablemente necesitemos alguna utilidad especial para arrancarlo. Existen utilidades en Internet para realizar esta labor.

EL DIRECTORIO PARA LOS ARCHIVOS DE INICIO DE SESIÓN.

El archivo de inicio de sesión es leído desde un directorio específico del servidor que valida el inicio

de sesión. Este directorio suele ser %systemroot% \system32\Repl\Import\Scripts aunque se puede modificar. Hay que tomar varias precauciones para que este mecanismos funcione:

ð El usuario debe tener permiso de lectura en el fichero y directorio de los archivos de inicio. Sobre una partición FAT, los usuarios del dominio normales no tienen permiso de lectura,

net use z: \\correo\usuarios

z:

cd usuario18

mail.exe.

luego si hemos instalado el sistema sobre una unidad FAT conviene, mover el directorio de inicio de sesión a una partición NTFS.

ð Si tenemos dos o más controladores de dominio, los archivos de inicio de sesión deben hallarse en todos ellos. Se puede proceder copiando manualmente los ficheros o utilizando el servicio de aplicación de directorios. Este servicio tiene como uso principal la copia automática de los archivos de inicio entre los servidores del dominio.

ð Una vez que se ha modificado un archivo y se está utilizando el servicio de duplicación de directorios, el usuario no debe iniciar sesión hasta que el nuevo archivo se haya copiado en todos los controladores del dominio. Esto se puede demorar algunos minutos.

LOS PERFILES DE USUARIO EN NT.

Los perfiles de usuario de NT permiten especificar las opciones del entorno para cada usuario de Windows NT. En Windows 3.x estas opciones habitualmente se guardaban en archivos .ini que eran archivos de texto normalmente compartidos por todos los usuarios de la aplicación. En NT todas las opciones y configuraciones del sistema y de las aplicaciones se guardan en el registro. El registro es una base de datos jerarquizada donde se guarda toda la información de configuración. En NT existe un registro completo para el sistema y uno para cada uno de los usuarios que han iniciado sesión en el sistema, que son los llamados perfiles de usuario.

Cuando un usuario inicio sesión por primera vez en NT el sistema crea un registro personalizado

para el usuario. Si no se ha definido previamente u perfil para el usuario, el sistema utilizará una copia del perfil de usuario por defecto. Tanto los perfiles de usuario como el perfil de usuario por defecto se puede editar para establecer de antemano las opciones del entorno de usuario.

PERFILES DE USUARIO FRENTE A PERFILES OBLIGATORIOS.

Cuando un usuario inicia sesión en un NT el sistema busca su perfil. Este perfil existirá si el usuario ya ha iniciado anteriormente sesión en NT. En caso de que no tenga perfil utiliza una copia del perfil de usuario por defecto. Las modificaciones que realice el usuario en su entorno se guardarán en esta copia del perfil.

Se puede modificar este mecanismo para asignar un perfil concreto al usuario. Esto se hace con el administrador de usuarios, que permite asignar un fichero de perfil, creado con el editor de per files, al usuario. Se pueden elegir dos tipos de perfiles:

ð perfil de usuario. El sistema crea un perfil para el usuario basándose en este fichero. Este proceso sólo se realiza la primera vez que el usuario inicio sesión en la máquina.

ð perfil obligatorio. El sistema crea un perfil para el usuario basándose en este fichero cada vez que el usuario inicia sesión en el sistema, de manera que el usuario pierde la configuración. Esto permite que el usuario parta de un entorno estándar cada vez que inicia sesión.

Se pueden eliminar perfiles antiguos de usuarios del sistema. Para ello, debemos abrir el menú ***Opciones/Eliminar perfil*** del icono ***Instalación de Windows*** en la carpeta principal del administrador de programas.

PERFILES EN NT 4.0

En NT 4.0 se han introducido algunos cambios en la estructura de perfiles:

ð Los perfiles en 3.X constaban sólo de un archivo, que era la clave del registro correspondiente al usuario HKEY_USERS\Usuario. En NT 4.0 además el perfil cuenta con una estructura de directorios para soportar el nuevo entorno de escritorio..

ð En NT 4.0 desaparece la herramienta "Editor de perfiles": La funcionalidad de esta herramienta se ha integrado en el Panel de control, en el icono Sistema, y en el Editor de Directivas del Sistema.

ð El nuevo sistema de directivas del dominio centraliza la configuración de seguridad de las estaciones, servidores, usuarios y grupos de usuarios del dominio.

TIPOS DE PERFILES DE USUARIO

En NT se pueden definir tres tipos de perfiles de usuario:

ð **Loc**al. Este perfil es específico del ordenador en el que se ha creado. El usuario sólo puede acceder al perfil local al iniciar sesión interactiva en el ordenador en el que reside el perfil.

ð **Móv**il. Este tipo de perfil puede ser usado por el usuario en cualquier NT del dominio. Es parecido al perfil móvil de Windows 95, pero es más completo.

ð **Obligator**io. Son perfiles móviles que el usuario no puede modificar. Normalmente son asignados a un usuario o grupos de usuario por el administrador.

En el perfil de NT 4.0 se guardan opciones como:

ð Todas las opciones definidas por el usuario en el explorador de NT

ð Las opciones de la barra de tareas.

ð Las opciones de impresión de red.

ð Las conexiones de red persistentes.

ð Algunas configuraciones de los accesorios y el sistema de ayuda.

ð Las opciones de las aplicaciones Win32

EL DIRECTORIO DE PERFILES EN NT

El directorio \Winnt\Profiles almacena los perfiles locales para cada usuario, en directorios separados cuyo nombre se crea a partir del nombre del usuario. Este directorio contiene además un perfil por defecto, en *Default Us*er, que se aplica a todo usuario que inicia sesión interactiva por primera vez< y no dispone de perfil, y un directorio llamado *All Users* que es accesible dentro del elemento programas del menú de inicio de todos los usuarios que inician sesión en el sistema. Esta carpeta guarda las carpetas de programas comunes a todos los usuarios.

En el directorio del perfil se almacena:

ð Un fichero con las claves del registro correspondientes al usuario. Este fichero se llama

NTUser.dat

ð Un fichero log, que mantiene los cambios efectuados en el registro. Se llama NTUser.dat.log. Cuando el usuario cierra sesión, el fichero NTUser.dat se actualiza con los cambios introducidos en NTUser.dat.log. En el caso de que existan problemas al actualizarel fichero NTUser.dat, los cambios se actualizarán en el siguiente inicio de sesión.

ð Directorios de datos, enlaces directos y aplicaciones, como son el Escritorio, carpeta Personal, carpeta Favoritos, carpeta Enviar a y otras carpetas ocultas..

PERFILES MÓVILES

Los perfiles móviles de NT 4.0 son más sofisticados que los perfiles que introdujo NT 3.X.

Los perfiles móviles de NT 4.0 permiten mantener de forma centralizada y sincronizada las preferencias y opciones del entorno de un usuario. Cuando un usuario inicia sesión en NT el sistema comprueba si el usuario dispone de un perfil móvil: Esto lo averigua buscando en la información de la cuenta del usuario. Si el campo "Directorio del perfil" tiene asignado un directorio, NT sabe que el usuario tiene un perfil móvil. Una vez que NT ha identificado un perfil como móvil, copia el perfil completo desde el servidor hasta el directorio \Windir\profiles local. El usuario puede modificar y usar su entorno. Al cerrar la sesión, el perfil central se actualiza con los cambios introducidos por el usuario.

CREACIÓN DE UN PERFIL EN NT 4.0

El método de creación de perfiles ha variado respecto a NT 3.X. En NT 4.0 ya no existe el editor de perfiles. La labor realizada por esta herramienta se ha sustituido por el icono de sistema del panel de control y por el editor de directivas del sistema POLEDIT.EXE.

Los pasos a seguir son sencillos:

ð Si vamos a mantener un gran grupo de perfiles conviene crear un recurso compartido de tipo unidad de red en un servidor adecuado. No es necesario que sea el controlador de dominio.

Por ejemplo:

\\servidor\perfiles

ð Configuramos la seguridad del recurso para que los usuarios tengan acceso a su perfil.

ð Iniciamos sesión con una cuenta con privilegios de administrador.

ð Modificamos el entorno(opciones, accesos directos, etc)

ð Ahora se abre el icono Sistema del Panel de Control, en la pestaña Perfiles de usuario..

ð Se selecciona el perfil de l usuario actual y se pulsa ***"Copiar a*** "

ð El botón ***"permitir usar*** a" indica a los usuarios o grupos de usuarios que se les permite usar el perfil. Este botón se usa con perfiles asignados a grupos del tipo obligatorio, ya que si un usuario no pertenece a un grupo que tenga permiso para usar el perfil, no podrá cargarlo.

ð Se copia el perfil al servidor, indicando la ruta al directorio que contiene el perfil. Por ejemplo: \\servidor\Perfiles\NombreUsuario

ð Se abre el administrador de usuarios y se edita la propiedad ***Perfil del usuar***io. En el directorio del perfil se escribe la ruta al perfil..

ð Se comprueba ahora en el ***Panel de Control\Sistema\Perfiles*** que se trata de un perfil móvil

PERFILES OBLIGATORIOS

Para asignar un perfil a un usuario de manera que el usuario no pueda actualizar el perfil con los cambios introducidos se utiliza el perfil obligatorio. Los perfiles obligatorios ayudan al administrador a gestionar los perfiles, ya que aseguran que el usuario cada vez que inicia la sesión encuentre un entorno coherente. Esto suele ser necesario con usuarios inexpertos o por simples motivos de seguridad..

Cuando el administrador debe mantener una gran cantidad de cuentas de usuarios, puede asignar perfiles obligatorios a un grupo. Por ejemplo, puede crear un perfil para los usuarios del grupo Contabilidad, de manera que todos ellos tengan el mismo perfil. Para crear un perfil obligatorio hay que:

ð Renombrar el fichero NTUser.dat a NTUser.man.

ð Indicar la extensión man en el directorio del perfil

\\servidor\Perfiles\NombreUsuario.man

Este último paso impide en NT 4.0 que el usuario pueda iniciar sesión con el perfil cache si el perfil principal no está disponible (el servidor de perfiles está fuera de servicio).

EL EDITOR DE DIRECTIVAS DEL SISTEMA POLEDIT.EXE

Las directivas del sistema permiten a los administradores controlar la configuración y la capacidad de modificar el entorno por parte de los usuarios. Esto puede ser realizado de una forma centralizada para todo el dominio sobre:

ð **Ordenador**es. Se puede modificar la configuración predeterminada de los servidores y estaciones de trabajo.

ð **Usuari**os. Se puede eliminar la capacidad de un usuario para acceder a partes delicadas de la configuración del sistema, como es la configuración de red o partes del escritorio de NT.

ð **Grup**os. Se pueden asignar configuraciones para grupos de usuarios, lo que simplifica notablemente la administración del dominio.

FUNCIONAMIENTO DE LAS DIRECTIVAS

El modo de trabajo de las directivas del sistema consiste en modificar ciertas claves del registro, que son las que cierran el paso a las partes del registro más sensibles. Las herramientas de administración y el panel de control utilizan estas claves para permitir o denegar el acceso del usuario para la modificación de estas partes. Cuando se manejan directivas del sistema y perfiles de usuario hay que tener en cuenta que:

ð Las directivas del sistema complementan a los perfiles, ya que también añaden claves al registro. El perfil del usuario normalmente almacena información de configuración que no compromete la seguridad del sistema.

ð Las directivas del usuario se aplican añadiendo las claves **después** de haber cargado el perfil de usuario. Esto permite que independientemente de la configuración almacenada en el perfil del usuario, se puedan aplicar las restricciones de seguridad necesarios para el usuario.

Las directivas del sistema por tanto se aplican añadiendo o alterando las claves del registro tras la

carga del perfil..

CREACIÓN DE LAS DIRECTIVAS DEL SISTEMA PARA UN DOMINIO

La herramienta que permite modificar las directivas del sistema es el Editor de Directivas del sistema POLEDIT.EXE. Las directivas del sistema se pueden aplicar sobre el sistema actual, aunque cuando realmente se saca provecho de las directivas del sistema es cuando se definen directivas para un dominio completo.

Crear y modificar directivas para un dominio completo es sencillo. Para ello se deben seguir estos pasos:

ð Se crea una nueva directiva con el menú ***Archivo\nueva directiva*** del editor de directivas.

ð Se modifica convenientemente la directiva, añadiendo usuarios, grupos y computadoras.

ð La directiva se guarda en el fichero ntconfig.pol. Este fichero se debe guarda en el directorio de archivos de inicio de sesión (scripts) de todos los controladores de dominio. Para hacer esto se procede según se explicó con los archivos de inicio de sesión. Normalmente esto implica activar el Servicio de Duplicación de Directorios.

MODO DE FUNCIONAMIENTO DE LAS DIRECTIVAS.

El editor de directivas trabaja modificando las claves del registro. Para ello al crear una nueva directiva el editor carga desde unas plantillas un conjunto de directivas. Por defecto, el editor de directivas dispone de tres plantillas:

ð **common.a**dm. Contiene configuración común a NT 4.0 y Windows 95

ð **winnt.a**dm. Contiene configuración sólo de Windows NT.

ð **windows.a**dm. Contiene configuración sólo de Windows 95. Esta plantilla debe añadirla manualmente un administrador desde el subdirectorio \Windir\inf.

El árbol de directivas muestra conjuntos de directivas que se pueden activas. Cada una de las directivas puede tener un estado:

ð **Activado** *(casilla marcad*a). El editor de directivas modificará convenientemente las claves del registro para aplicar la directiva.

ð **Desactivado** *(casilla en blanco).* El editor de directivas modificará convenientemente las claves del registro para no aplicar la directiva.

ð **Sin cambios** *(casilla en gris*). Es editor de directivas no realizará ninguna modificación en el registro.

El ejemplo más sencillo es la directiva que indica el protector de pantallas que debe usar un usuario. Por defecto el usuario utiliza el protector de pantallas que dicta su perfil, que puede haber sido fijado por el propio usuario, residir en un perfil móvil, en un perfil obligatorio o haber sido creado por defecto automáticamente. Al activar esta directiva se puede modificar el comportamiento, obligando a un usuario a utilizar otro protector de pantalla (quizás el que tiene el logotipo corporativo y obliga a usar contraseña). En este caso de no activarse la directiva se utilizaría la del perfil.

LOS ARCHIVOS DE PLANTILLAS DE DIRECTIVAS

Los archivos de plantillas son simples archivos de texto que se pueden editar. Por ejemplo, una sección ilustrativa del archivo winnt.adm es:

```
CATEGORY !!UserProfiles
KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\winlogon"
POLICY !!DeleteRoamingCachedProfiles
VALUENAME "DeleteRoamingCache"
PART !!DeleteCache_Tip1 TEXT END PART
PART !!DeleteCache_Tip2 TEXT END PART
END POLICY
```

Donde las cadenas de caracteres que empiezan por !! se expanden según:

```
DeleteRoamingCachedProfiles="Eliminar copias en el caché de
perfiles móviles"
DeleteCache_Tip1="Cuando los usuarios con perfiles móviles
cierran
```

la sesión,"

DeleteCache_Tip2="se elimina el perfil en el caché local para

ahorrar espacio.".

Se observa que la clave corresponde a KEYNAME y el valor de la clave a VALUENAME.

El formato de las directivas está previamente definido en la documentación de Microsoft. (Kit de Recursos y de Programación).

DIRECTIVAS PARA SISTEMAS, USUARIOS Y GRUPOS

Se pueden crear tres tipos de directivas:

ð **Directivas para sistemas.** Permiten gestionar fácilmente varios ordenadores, ya que la información almacenada en las directivas del dominio son asumidas por todos los sistemas cuando se incorporan al dominio al arrancar.

ð **Usuari**os. Es el modo más sencillo de gestionar la seguridad de un usuario.

ð **Grupos.** Cuando el número de usuarios es grande se puede dividir la configuración en grupos.

Hay que tener en cuanta que las directivas se aplican de modo acumulativo. Si un usuario pertenece a varios grupos para los que se han fijado directivas, el orden de aplicación se obtiene según se halla fijado en el cuadro de diálogo ***"directivas de grupo***"

EL SERVICIO DE DUPLICACIÓN DE DIRECTORIOS.

El servicio de duplicación de directorios se diseñó principalmente para poder duplicar de forma sencilla ficheros a lo largo de todo el dominio. Tiene grandes limitaciones, ya que no es un sistema que permita duplicar unidades compartidas para la ejecución de programas por ejemplo, sino simplemente algunos archivos como son los archivos de inicio de sesión.

La configuración típica del servicio de duplicación de directorios se da normalmente cuando disponemos de un controlador principal de dominio y varios controladores secundarios. Para instalar el servicio de duplicación en todos los controladores del dominio podemos realizar el siguiente procedimiento, que está dividido en tres fases:

1º) Se debe crear una cuenta para usar con el servicio de duplicación. Para ello abrimos el

administrador de usuarios para el dominio y realizamos los siguientes pasos:

− Creamos una cuenta de nombre duplicador (por ejemplo)

− Le asignamos una contraseña

− Desactivamos la casilla que obliga al usuario a cambiar la contraseña en el siguiente inicio de sesión.

− Activamos la casilla para que la contraseña nunca caduque..

− Le añadimos a los grupos Operadores de copia y duplicadores, y aceptamos este usuario.

− Seleccionamos en el menú ***Directivas/Derechos de usuario***. Dentro de este cuadro de diálogo mostramos las directivas avanzadas y seleccionamos *Iniciar sesión como servic*io. Añadimos el usuario duplicador al grupo de usuarios de esta directiva. En NT 4.0 esta opción también la realiza el servicio de duplicación al configurarlo en el ***Panel de Control\Servicios***.

2º) Se configura el servidor de exportación. El servidor de exportación será la máquina que contenga todos los ficheros de inicio. Para ello se abre el administrador de servidores y se selecciona Propiedades/ Duplicación en el servidor de exportación. Ahora se configura el servidor:

ð Se selecciona exportar directorios.

ð Se añade a la lista el nombre del dominio, con el botón de ***Agregar***.

ð Se configura el directorio de exportación, por ejemplo:

%system_root%\system32\repl\export.

ð Hay que asegurarse que este directorio existe y que tiene los permisos necesarios.

ð En el cuadro de diálogo ***Administar directorios exportados*** se añade el directorio **scripts.**

ð Para mayor rapidez en la transferencia de ficheros de inicio no marcar la casilla *Esperar hasta estabiliza*do.

3º) Se configuran los servidores de importación. Cada controlador secundario se debe configurar para que importe los ficheros de inicio de sesión. Para ello desde el administrador de servidores se selecciona Propiedades/ Duplicación en todos los controladores del dominio, incluyendo el principal y se configuran:

ð Se seleccionan importar directorios.

ð Se añade a la lista el nombre del dominio.

ð Se configura el directorio de exportación, por ejemplo:

%system_root%\system32 \repl\import.

ð Hay que asegurarse que este directorio existe y que tiene los permisos necesarios.

ð Se añade el directorio **scripts** desde el cuadro de diálogo ***Administrar directorios importados***.

Una vez configurados los servicios se reinician los servicios con el ***Panel de Control\Servicios***.

Si todo funciona correctamente, en los servidores de importación aparecerán mensajes de sincronización correcta en el cuadro de diálogo ***Administrar directorios importados***.

EL SISTEMA DE FICHEROS DISTRIBUIDOS DFS

El servicio DFS permite crear un sistema de ficheros distribuidos que puede ser utilizado por máquinas NT 4.0 y Windows 95.

MEMORIA VIRTUAL

La versión actual de NT está desarrollada para entornos de ejecución de 32 bits. En estos entornos del hardware (microprocesador y gestor de memoria virtual) permite que los procesos puedan acceder a espacios de memoria separados de 4 Gigabytes. NT dispone de un gestor de paginación que permite utilizar múltiples particiones no dedicadas de diferentes discos para almacenar páginas de memoria, de manera que la cantidad de memoria que usan los procesos puede ser mayor que la cantidad de memoria física instalada en el sistema. Este mecanismo es flexible (permite utilizar múltiples particiones para almacenar ficheros de intercambio) y dinámico, que el tamaño de los ficheros de intercambio crece y decrece según lo necesitan los procesos.

El gesto de memoria permite a NT mapear ficheros en la memoria de los procesos, lo que permite a los procesos y aplicaciones de usuario manipular estos ficheros como si estuviesen en el espacio de memoria del proceso, de manera que es el gestor de memoria el encargado de actualizar los cambios introducidos sobre el fichero. Este mecanismo permite además una carga muy rápida de los

ficheros ejecutables.

ENTRADA Y SALIDA EN NT

El sistema de entrada y salida en NT gobierna todas las operaciones realizadas sobre ficheros y dispositivos. Está compuesto por un administrador de entrada y salido sobre el que se montan los diferentes módulos:

ð **El gestor de sistemas de ficheros instalables** permita al sistema acceder a múltiples tipos de sistemas de ficheros, entre ellos VFAT (Compatible con el FAT de MSDOS y Windows 95), HPFS (de OS/2), CDFS (para acceder a unidades CD−ROM) y el nuevo NTFS. Que tiene nuevas características avanzadas (seguridad, soporte para atributos complejos, soporte para discos de gran tamaño, etc.)

ð **El redirector de r**ed, que permite operar sobre sistemas de ficheros remotos, utilizando diversos protocolos de red.

ð **El gestor de dispositivos físic**os, que permite al sistema comunicarse con los dispositivos directamente.

ð **El administrador de cac**hé, que permite optimizar el acceso a los ficheros y dispositivos. Este gestor es común tanto para los diferentes sistemas de ficheros como para el redirector de red.

EJECUCIÓN DE APLICACIONES EN NT

Todas las aplicaciones de usuario se ejecutan en NT dentro de un subsistema de entorno. Los subsistemas de entorno en NT son procesos que proporcionan a las aplicaciones las API necesarias para su ejecución. Los subsistemas de entorno son los encargados de llamar a los servicios nativos del núcleo de NT. Este esquema de ejecución de aplicaciones permite ejecutar aplicaciones preparadas para diferentes entornos. El principal entorno de ejecución de aplicaciones lo compone el subsistema de entorno Win32. Este subsistema tiene dos misiones: ejecutar las aplicaciones Win32 y servir de soporte para otros subsistemas.

Las aplicaciones escritas para MSDOS se ejecutan dentro de otro subsistema, el llamado entorno de máquinas DOS virtuales (Virtual Dos Machines) que proporciona el entorno completo que ofrece

una máquina corriendo el sistema operativo MSDOS. Hay que hacer notar que este subsistema supervisa la ejecución de todas las aplicaciones MSDOS. El entorno de máquinas virtuales es capaz de emular parte de la funcionalidad que soporta el hardware típico de los entornos MSDOS, como es el acceso a la memoria de vídeo, aunque la emulación no es completa, por lo que algunas operaciones no son posibles. El soporte para estas operaciones y para la emulación es proporcionado por los controladores de dispositivo. Dependiendo de la potencia del controlador, la emulación del hardware será más o menos completa.

El subsistema Win16 está soportado por el subsistema VDM. En general todas las aplicaciones de 16 bits se ejecutan en la misma máquina virtual, por motivos de compatibilidad, aunque se puede ejecutar una aplicación Win16 en un espacio de memoria separado. Esto es especialmente útil en aquellas aplicaciones que no se comportan correctamente, ya que permite seguir ejecutando las demás aplicaciones de Win16 en caso de fallo de la aplicación. Las aplicaciones de Win32 corren en su propio espacio de memoria, por lo que en caso de fallo de una aplicación el subsistema Win32 la puede eliminar sin afectar a las demás..

El protocolo TCP/IP en Windows NT

INTRODUCCIÓN

El protocolo TCP/IP nación de los trabajos del ARPA (Advanced Research Project Agency) del Departamento de Defensa de los EEUU, durante las décadas de los 60 y 70. A través de las universidades y centros de investigación se trató de construir una red que fuese capaz de resistir las caídas parciales de la misma (por ejemplo en caso de guerra). Así surgió ARPANET, la primera red de intercambio de paquetes.

En 1974 V. Cerf y R. Kahn propusieron un nuevo conjunto de protocolos básicos de red que solventaban gran parte de los problemas de los protocolos usados en ARPANET. Así se pusieron los cimientos de los protocolos IP (Internet Protocol) y TCP (Transmission Control Protocol). En 1980 se comenzó la migración de los aproximadamente 100 servidores que formaban la red ARPANET a los nuevos protocolos. En 1983 el Departamento de Defensa estandarizó el

protocolo TCP/IP como protocolo básico de red. Rápidamente otras agencias del gobierno adoptaron el protocolo, lo que obligó a las empresas proveedoras de equipos a implementarlo en sus sistemas operativos y equipos de comunicaciones. Además el Departamento de Defensa impulsó el protocolo TCP/IP al recomendar a la Universidad de Berkeley la inclusión del protocolo en la distribución BSD 4.2 del UNIX.

EL PROTOCOLO TCP/IP FRENTE A OTROS PROTOCOLOS

El sistema operativo NT da soporte directamente a tres protocolos de red: NETBEUI, usado en las redes de Microsoft e IBM principalmente, IPX/SPX, usado en las redes Novell Netware y el TCP/IP, parte básica de las redes UNIX, y principal protocolo de la Internet. Cada uno de estos protocolos tiene sus propias ventajas e inconvenientes. De un modo general se recomienda cada uno de estos protocolos:

ð **Netbeui.** Para compartir ficheros e impresoras en redes sencillas. Para este tipo de redes se muestra muy eficaz, dada su prácticamente nula necesidad de configuración. No es encaminable.

ð **IPX/S**PX. De aplicación en redes en las que existan servidores Novell Netware. Tiene un buen rendimiento en ficheros e impresión y poca dificultad de administración.

ð **TCP/**IP. Es el que peor rendimiento ofrece para uso en ficheros e impresión, pero es el que presenta mayores herramientas para crear grandes redes de ordenadores. Es encaminable y es imprescindible en Internet. Microsoft ha implementado todas las características de Netbios dentro del protocolo TCP/IP. Es el que obliga al mayor esfuerzo administrativo.

ELEMENTOS DEL PROTOCOLO TCP/IP.

Una red de ordenadores está compuesta de dos partes: la red física en sí y el protocolo que utilizan los ordenadores para comunicarse entre sí. La red física está compuesta normalmente de una serie de subredes, a las que se conectan los diferentes equipos (ordenadores, impresoras...). Esta red puede tener una topología muy variada. Actualmente existen tres tipos de topologías:

Ethernet, que es del tipo bus, Token Ring, que tiene topología de testigo y utiliza topología de bus con paso de testigo. El protocolo TCP/IP fue desarrollado inicialmente para Ethernet , pero

admite sin problemas las otras dos tecnologías. Actualmente se está imponiendo la tecnología Ethernet en las redes pequeñas, sobre todo sobre cableado de par trenzado (10 Base T), y por su bajo coste y buen rendimiento..

Normalmente una red típica estará compuesta por una serie de ordenadores conectados entre sí, además de impresoras y otros elementos de la red.

Cada ordenador tendrá al menos una tarjeta de red. Esta red se puede unir a otras redes o al resto de la Internet a través de puentes, encaminadores y otros tipos de enlaces. El protocolo TCP/IP permite identificar cada elemento de la red y proporciona los mecanismos para el intercambio de información entre estos elementos.

El protocolo TCP/IP está formado por un protocolo genérico de envío y recepción de paquetes, llamado IP por ser el protocolo nativo de Internet (Internet Protocol), sobre el que se construyen otros protocolos de mayor nivel. El más importante de ellos, el protocolo TCP (Transmission Control Protocol), da nombre, junto con el IP, al protocolo TCP/IP. A su vez estos protocolos pueden incluir subprotocolos dentro de ellos. Esto se verá claramente en el protocolo TCP.

Cada paquete enviado a través de la red tiene un formato específico. Si usamos el protocolo Ethernet de transmisión, cada paquete está compuesto de una cabecera Ethernet y de un campo de datos. La cabecera Ethernet origen y la de destino. Las direcciones Ethernet están compuestos por un número de 6 bytes. Este número es asignado a cada tarjeta de manera única. Cuando dos ordenadores de la red deben intercambiar paquetes Ethernet, deben escribir la dirección origen y destino en ellos. Como en una red Ethernet los paquetes viajan por toda la red, las tarjetas de red sólo atienden a aquellos paquetes cuya dirección destino coincide con su dirección Ethernet. Existe un método para que una tarjeta envíe paquetes a todos los ordenadores. Este mecanismo es conocido como difusión de paquetes (Broadcast). Cuando la dirección destino son 6 bytes a 0 [cerciorarse si son a 0 o a 255], todas las tarjetas procesan el paquete. Este mecanismo es usado habitualmente por los protocolos de red para comunicarse dentro de una red local, pero tiene el inconveniente de que sobrecarga la re, por lo que debe ser evitado en la medida de lo posible. Los

protocolos token ring y token bus se comportan de modo análogo. El campo de datos contiene el paquete IP. Cada paquete IP está compuesto de una cabecera y un campo de datos. La cabecera está compuesta de los siguientes campos:

Campo **Tamaño**

Explicación

Versión **4 Número de versión del protocolo IP (actual=4)**

IHL **4 Longitud de la cabecera, en palabras de 32 bits**

Tipo de servicio **8 Indica cómo debe ser tratado el paquete durante la transmisión (prioridad fiabilidad)**

Longitud total **16 Longitud del paquete en octetos**

Identificación **16 Usado en la fragmentación de paquetes.**

Flags **3 Permiten o inhiben la fragmentación**

Desplazamiento de Fragmento

13 Posición del fragmento en el paquete original.

IP Origen **32 . IP del ordenador origen. Son 4 octetos**

IP Destino **32 IP del ordenador destino. Son 4 octetos.**

Opciones **Para incluir datos propios de los protocolos. Tamaño variable.**

Relleno **Para completar la cabecera a plabras de 32 bits.**

TTL **8 Tiempo de vida del paquete. Es un número que se decrementa cuando el paquete por un**

encaminador. Si se hace 0 se descarta el paquete, Recomendable que sea mayor de 64 en Internet.

Protocolo **8 Identifica el tipo de protocolo a usar (TCP,UDP,...)**

Suma de control 16 Verifica la integridad de la cabecera.

En el origen del protocolo TCP/IP, el TCP era el protocolo usado, pero luego se extendió el rotocolo IP con nuevos protocolos como son el Protocolo de Control de Mensajes de Internet

(CMP), los protocolos de resolución de direcciones directo e inverso (ARP y RARP) y el rotocolo de Datagramas de Usuario (UDP).

EL SISTEMA DE DIRECCIONES DEL PROTOCOLO IP.

A cada servidor de la red TCP/IP se le asigna al menos una dirección IP, que es un número e 4 octetos. En la red Internet no hay dos ordenadores con el mismo número IP. En caso de necesidad se pueden asignar más números IP a ese ordenador. Además cada dirección IP tiene un nombre asociado. Ese nombre está formado por el nombre del servidor, que es único dentro de una subred, y por el nombre del dominio, que identifica a la subred dentro del conjunto de las subredes de Internet. La forma de asignar IP, nombres y nombres de dominio en Internet sigue una serie de criterios que permiten el encaminamiento de los paquetes IP por la red y la traducción de nombres de ordenadores en números IP.

En Internet hay tres tipos de organizaciones de IP:.

ð **Organizaciones tipo** A. El primer octeto del IP es el mismo para toda la organización. La organización asigna del IP es el mismo para toda la organización. La organización asigna al resto de los octetos a cada IP de su organización. La organización dispone de [calcular 256 3] direcciones para asignar. Este tipo de organizaciones sólo se asignan a países.

ð **Organización tipo** B. Los dos primeros octetos del IP están fijos. La organización dispone de 65536 direcciones IP para asignar. Suelen ser organizaciones de tamaño medio (universidades, grandes empresas).

ð **Organización tipo C.** Se fijan los tres primeros octetos, dejando 256 posibles direcciones. Se utilizan en pequeños proveedores de servicios Internet (ISP).

RESOLUCIÓN DE NOMBRE EN EL PROTOCOLO IP.

Cuando dos ordenadores se quieren comunicar mediante el protocolo IP, deben conocer ambos sus respectivas direcciones IP. Por ejemplo, si se desea conectar desde un ordenador a otro mediante un cliente del protocolo de transferencia de ficheros (FTP), debemos suministrar al cliente la dirección IP de destino. Dado que los números IP son difíciles de recordar, en Internet se dispone

de un mecanismo que permite asociar nombres significativos a cada IP. Por ejemplo, el servidor de FTP de una organización podría llamarse ftp.organizacion, donde organización es el nombre del dominio de dicha organización. Se puede emplear el archivo HOSTS de cada servidor para incluir en él una lista de direcciones IP con su nombre correspondiente. De esta manera se puede proporcionar al cliente FTP el nombre ftp.organizacion como IP de destino, y el protocolo IP se encarga de obtener el número IP. A este mecanismo se le llama resolución de nombres.

Dado que mantener una lista de direcciones IP y nombres es complicado (habría que duplicar los archivos HOSTS por todos los servidores), en Internet se ha creado un mecanismo de resolución de nombres automático: el Servicio de Nombres de Dominio (DNS). En cada dominio hay al menos un servidor de nombres de dominio, que mantiene una lista de todas las direcciones IP del dominio y sus nombres asociados. Incluso podemos incluir varios nombres para una misma direccion IP (por ejemplo en los servidores de FTP y WWW de la organización residen en el mismo servidor, podemos incluir los nombres ftp.organizacion y www.organizacion en el servidor de nombres. Además en Internet, los servidores de nombres están organizados de una forma jerárquica, de manera que si el nombre buscado no pertenece al dominio del ordenador, el servidor DNS puede buscar en otros servidores DNS de otros dominios hasta encontrar el servidor DNS del dominio destino, y de él recuperar la dirección IP de destino. Este mecanismo es generalmente muy rápido (menor que unos 2 segundos la búsqueda con éxito y unos 10 o 20 una búsqueda con resultado negativo), ya que los servidores DNS poseen mecanismos de caché.

EL MECANISMO DE DIFUSIÓN (BROADCAST) EN EL PROTOCOLO IP:

El protocolo IP al igual que el protocolo Ethernet también dispone de un mecanismo de difusión (broadcast), que permite enviar paquetes desde un ordenador a todos los ordenadores de la red. Cada tipo de subred (A,B o C)tiene una máscara de subred asociada (255.0.0.0 para la A, 2555.2555.0.0 para la B y 255.255.255.0 para la C) que determina las direcciones IP que escuharan los paquetes de difusión. El protocolo de difusión es ampliamente usado por Netbios sobre TCP/IP en la implementación de Microsoft, lo que permite emular al protocolo TCP/Ip de

Windows el comportamiento del protocolo Netbeui.

El protocolo de difusión de paquetes tiene dos grandes desventajas: la primera es que sobrecarga la red. Por ello en las redes basadas en Windows se introduce el protocolo WINS, que intenta evitar en la medida de lo posible el envío de paquetes de difusión. La segunda desventaja es que los puentes y encaminadores que comunican las subredes, si entienden el protocolo IP, no permiten el paso de paquetes de difusión..

IMPLEMENTACIÓN DEL PROTOCOLO TCP/IP EN NT

La implementación del protocolo TCP/IP en NT persigue dos metas: implementar completamente el protocolo TCP/IP en NT, tanto a nivel de protocolos (IP,TCP;UDP,etc) como la inclusión de los servicios más habituales (FTP, TELNET (Cliente sólo), SNMP y otros). Por otro lado permite utilizar el protocolo TCP/IP como único protocolo de la red, ya que los servicios de Netbios sobre TCP/IP permiten la compartición de ficheros e impresoras en la red Windows. La mayor parte de los clientes TCP/IP tienen versión para NT. Se está haciendo un gran esfuerzo a su vez para dotar a NT de todos los servidores típicos de Internet. Hay servidores de dominio público de FTP, DNS, Gopher, TELNET, SMTP, POP3 Y WEB, aparte de las propias incluidas en el NT Server. además existen versiones comerciales de dichos servidores, normalmente más potentes y seguras.

CONFIGURACIÓN DEL PROTOCOLO TCP/IP EN NT.

Antes de proceder a la instalación del protocolo TCP/IP en **NT** hay que averiguar una serie de parámetros, que deben ser suministrados por el administrador de la red. Si en la red además existe un servidor DHCP probablemente no sea necesario conocer ningún parámetro, ya que el protocolo se configurará automáticamente. Para añadir el protocolo TCP/IP se pulsa el botón Agregar software dentro del cuadro de diálogo Red del Panel de Control:

En NT 3.51 debemos elegir la opción Protocolo TCP/IP y elementos relacionados. En este cuadro de diálogo nos aparecen las opciones que se pueden instalar. En Nt 4.0 se elige en Panel de control\Red\Protocolos\Agregar el Protocolo TCP/IP y elementos relacionados..

En este cuadro se pueden señalar las opciones a instalar. Las más comunes son las utilidades de

conectividad (clientes ftp, telnet, finger, etc.), y son básicamente las únicas necesarias. En este cuadro de diálogo también se puede seleccionar la configuración automática vía el protocolo DHCP. En NT 4.0 el cuadro de diálogo se ha modificado de manera que ahora la configuración del protocolo TCP/IP está organizada por bloques funcionales. En el caso de configuración manual debemos conocer una serie de parámetros. El primero es la dirección IP del ordenador. En NT se puede asignar una dirección IP a cada adaptador de red instalado, e incluso a un mismo adaptador se le pueden asignar varias direcciones IP. Esto último se usa en Internet para crear servidores virtuales. Luego se debe incluir una de las tres máscaras de subred posibles, para redes de tipo A, B o C. Si la red en la que se halla conectado el ordenador está conectada con otras redes vía una pasarela (gateway), que puede ser un puente o encaminador, hay que incluir su dirección en la casilla para puerta de enlace.

Si en la red hay servidores WINS, podemos incluir la dirección de un servidor WINS primario y otro secundario..

Si en la red hay un servidor DNS (obligatorio en las redes conectadas a Internet) podemos completar las opciones de DNS.

Como nombre de host, NT por defecto usa el de Windows, pero debería coincidir con el que se le ha asignado en el servidor de nombres. En la lista Orden de búsqueda del servicio de nombres de dominio debemos proporcionar una lista con las direcciones IP de los servidores de nombres que debe usar. Se pueden incluir servidores de nuestra red y de otras, aunque suelen ser más lentos.

Debemos añadir a la casilla nombre de dominio el nombre de dominio de la subred local. Si no se proporciona un dominio, el protocolo TCP/IP usa por defecto el dominio local.

Podemos añadir otros dominios para que se usen por defecto, añadiendo entradas a la lista orden de búsqueda del sufijo de dominio.

Se pueden configurar varias opciones avanzadas para cada adaptador de red o pulsando el botón ***avanzadas*** del cuadro de diálogo ***Configuración de TCP/IP***, en la sección Dirección IP..

También se puede activar el protocolo PPTP (Point to Point Tunneling Protocol) que es el

Protocolo de Túnel Punto a Punto. Este protocolo permite construir redes privadas seguras dentro de redes de transmisión públicas, siendo capaz de encapsular los diferentes protocolos de red empleados en NT, como son NETBEUI, TCP/IP y IPX/SPX. Este protocolo utiliza cifrado de los paquetes, y algoritmos de clave pública que hacen muy difícil examinar los paquetes enviados a través de una red como puede ser Internet.

En este cuadro se pueden:

ð Asignar múltiples direcciones IP a un mismo adaptador. Esto se usa cuando un mismo adaptador de red debe poseer varias direcciones IP. En Internet es muy común el asignar múltiples direcciones IP a un adaptador. El mejor uso de este mecanismo consiste en reservar una dirección IP y un nombre de ordenador para cada servicio Internet que se instale en el servidor. Si por ejemplo se planea instalar un servidor FTP y un servidor WWW sobre el servidor, se deben reservar dos direcciones separadas de la principal del servido, e instalar cada uno de los servicios en cada dirección. De esta manera es muy fácil

llevarse todo es servicio a un nuevo servidor cuando por sobrecarga del servidor no se puede hacer frente a las solicitudes efectuadas por los clientes de este servicio.

ð Añadir nuevas pasarelas o puertas de enlace para ese adaptador.

ð Activar el agente de Proxy WINS, para lo cual la red debe disponer de servidor WINS. Un agente de proxy WINS es un equipo que permite que otros equipos que no están configur ados para acceder a un servidor WINS puedan acceder a los nombres contenidos en ese servidor WINS. Normalmente esta situación se da cuando el servidor WINS está en una red remota, por lo que los equipos de la red local que no tienen activado el cliente WINS no pueden acceder a los nombres registrados en ese servidor. Al activar el proxy WINS las peticiones de búsqueda y registro de nombres Windows realizadas en modo local (vía broadcast) son atendidas y redirigidas sobre el servidor WINS por el servidor proxy WINS.

ð Configurar los parámetros de red de Windows, que funcionan con el protocolo Netbios sobre TCP/IP. El archivo

En NT 4.0 se ha introducido el agente Relé de DHCP. Normalmente el protocolo DHCP funciona sobre una red local, ya que se trabaja siempre en modo de difusión de paquetes (broadcast). En este modo los paquetes no pueden saltar los encaminadores, salvo que éstos soporten el protocolo de reenvío de paquetes BOOTP. Si es necesario que en una red se tenga acceso a un servidor DHCP remoto, se puede instalar un relé DHCP, que es un servicio que se conecta con un servidor DHCP remoto para realizar la configuración dinámica en la red local. Se pueden añadir en el cuadro de diálogo de Relé DHCP varios servidores DHCP, así como configurar los parámet ros de funcionamiento del relé.

En el cuadro de diálogo de ***Enrutamiento*** (encaminamiento) se puede activar el encaminamiento IP, si se disponen de 2 o más direcciones IP en el ordenador. Esta situación es habitual cuando se disponen de dos tarjetas de red, cada una conectada a una red física diferente..

Servicios de Internet / Intranets

NT es un sistema operativo con una gran capacidad para trabajar en red que le permite configurar de un modo simple y rápido una Intranet. El protocolo TCP/IP cuenta con una aceptación muy grande en la industria y se han desarrollado gran cantidad de estándares, protocolos y herramientas para él. Su difusión es tal que se está imponiendo prácticamente como el protocolo preferido por las empresas para el desarrollo corporativo. Debido a la potente implementación del protocolo TCP/IP en NT y al amplio número de herramientas que vienen incorporadas o que están disponibles desde otras compañías, se puede aprovechar este protocolo para crear una Intranet empresarial.

CREACIÓN DE UNA INTRANET

Para crear una Intranet se deben configurar correctamente los servidores y el protocolo TCP/IP, de manera que se anticipe al crecimiento de la red. Una intranet puede comenzar constando de un solo servidor NT con unas pocas estaciones de trabajo Windows. Al crecer la red puede ser necesario añadir más servidores para descargar de servicios a los ya existentes.

Para comenzar a construir la intranet hay que configurar un servidor NT Server. Los servicios que

hay que instalar en el servidor son:

ð La pila TCP/IP. Primero hay que asignar las direcciones IP a los diferentes ordenadores de la red. Para ello haremos uso de los rangos de direcciones privadas reservadas dentro del protocolo TCP/IP

IP inicial IP final Tamaño 10.0.0.0 10.255.255.255 Clase A

172.16.0.0 172.31.255.255 15 Clases B (15x64k)

192.168.0.0 192.168.255.255 Clase B

NOTA: Si estamos interesados en conectarnos con otra red, por ejemplo Internet o Infovía, conviene utilizar rangos de direcciones que no coincidan con esta red.

ð **Conviene agrupar las direcciones dentro del rango en paquetes de direccion**es. Por ejmplo se puede dividir el rango en tramos múltiplos de 16 o de 32 direcciones. Esto permite luego examinar la red con filtros basados en rangos de direcciones IP, utilizando herramientas como el monitor de red, incluido en System Management Server. Esto facilita además el trabajo con encaminadores y otros dispositivos de control de la red.

ð **Instalación de un dominio en el servidor.** Ya que vamos a dar servicios de red a la intranet, configuraremos el servidor como controlador de dominio. Luego añadiremos los servicios para trabajar como servidor de red Microsoft, incluyendo compartición de ficheros, impresoras, perfiles de usuarios, archivos de inicio de sesión, directivas y seguridad para el dominio, etc.

ð **Configuración del servidor como D**NS. El servidor DNS permite que el protocolo TCP/IP sea sencillo de manejar. Además de cara a la integración de la red con Internet, poseer un servidor DNS propio evita tener que alquilar este servicio al proveedor de servicios de Internet.

ð **Configuración de un servidor WI**NS. El servicio WINS es el servidor de nombres Internet para Windows y permite que el protocolo Netbeui sobre TCP/IP pueda trabajar de un modo más eficientes que la resolución de nombres Windows no se hace mediante difusión de paquetes (broadcast), sino conectando directamente con el servidor. Además la configuración y el mantenimiento son muy sencillos y prácticamente no consume recursos en los servidores. Para

configurar el servidor WINS consulte el capítulo *El servidor WIN.S*

ð **Configuración de un servidor W**eb. Dentro del servidor añadiremos una nueva dirección IP y a esta dirección le añadiremos como nombre www en el DNS. La técnica de asignar múltiples direcciones IP a un servidor permite que en el futuro se pueda migrar de manera muy rápida el servidor web u otros servidores de Internet a otras máquinas. Hay que tener en cuenta que cuando se configuran algunos servicios, hay veces que es obligatorio especificar direcciones IP, no nombres de servidores. El servidor Web será el almacén principal de documentación de la compañía. El mantenimiento del servidor IIS es realmente sencillo y potente. El uso del servidor por los usuarios es rápido y amigable. Se puede instalar el servidor en apenas unos minutos y la documentación se puede exportar fácilmente a formato HTML con la mayoría de las aplicaciones de última generación. Por ejemplo con los procesadores de texto nuevos suele bastar con guardar un documento como HTML. Para configurar el servidor IIS consulte el capítulo *El Servidor IIS y el IE*.

ð **Servidor de corr**eo. Es la piedra angular para la colaboración. Dado que NT no incluye un servidor de correo que soporte SMTP (en el kit de recursos hay uno pero no es muy bueno), hay que utilizar productos específicos. Se pueden elegir dos tipos de productos:

ð *Servidores de Trabajo en Grupo (Groupwi*se), al estilo de Microsoft Exchange o Lotus Notes. Estos servidores son herramientas muy potentes construidas alrededor de sistemas de mensajería y correo, que permiten compartir datos y correo entre los usuarios del grupo. Contienen gran cantidad de herramientas y utilidades.

ð *Servidores tradicionales de correo SM*TP. Son servidores que permiten enviar y recibir correo siguiendo los protocolos estándares de Internet. Los hay de dominio público como el IMS de EMWAC y los diversos servidores portados de UNIX (Sendmail y otros), aunque hay otros productos comerciales mucho más potentes, con herramientas de administración muy avanzadas.

ð **Servidor S**QL. Si se van a mantener bases de datos corporativas es momento de incluir un servidor SQL dentro de la Intranet. La mejor elección consiste en configurar un NT Server como Servidor y dedicarlo a estos menesteres. Por ejemplo, el SQL Server de Microsoft da un buen

rendimiento y se integra fácilmente con el servidor Web I IS de NT.

ð **Servidor de copias de seguridad**. Aunque NT dispone de un buen sistema de backup para los servidores que trabaja en modo local, se puede montar un servidor de copias de seguridad para que los usuarios puedan realizar sus propias copias de seguridad. Hay que productos que aportan gran flexibilidad a esta tarea, permitiendo copias desatendidas sin intervención del administrador.