1. PRIMEROS PASOS CON EL NUEVO SISTEMA

Ya al iniciar Windows NT, se observa que no tiene nada que ver con sistemas del tipo de Windows 95, sino que se trata de un sistema completamente independiente.

En la primera pantalla, ya se muestra como un sistema operativo multiusuario: es necesario identificarse.

Sin la autorización de acceso al sistema no existe ninguna posibilidad de trabajar con este sistema operativo.

Una vez arrancado el sistema, Windows NT mostrará su nuevo entorno de Windows 95.

Si ya ha trabajado con Windows 95, se orientará rápidamente. Para los usuarios que utilizan por primera vez este entorno ofrezco en las páginas siguientes un resumen de los aspectos más importantes.

1.1 El Nuevo entorno

Si anteriormente ha trabajado con Windows 3.11 o versiones anteriores de Windows NT, estos primeros pasos con el nuevo entorno le resultarán algo inusuales. Es inútil buscar el Administrador de programas de las anteriores versiones de Windows, así como el Administrador de archivos. En su lugar podrá ver un área de trabajo(escritorio) con iconos de programas. En el extremo inferior de la pantalla de presenta una barra gris con el botón *Inicio*. Esta barra se llama *barra de tareas.*

Con el fin de aclarar la idea del nuevo entorno, cabe señalar que no existe ninguna diferencia conceptual entre un archivo (gestionado con el Administrador de archivos) y un programa (gestionado con el Administrador de programas). En su lugar los exploradores muestran todos los archivos y programas conjuntamente.

Para iniciar un programa o abrir un archivo no hace falta saber donde es encuentra este exactamente dentro de la estructura de una unidad concreta. Simplemente basta con pulsar en el acceso directo a ese archivo situado en el escritorio o en el menú de *Inicio.*

El administrador de programas de Windows 3.x ha sido absorbido por la barra de tareas en Windows 95 y Windows NT 4.0. En el menú *Programas* encontrará tanto aplicaciones que se pueden iniciar directamente, como otros menús que recuerdan a los grupos de programas de las anteriores versiones Windows.

Sin embargo, el menú *Inicio* ofrece mucho más:

El menú *Documentos* muestra una lista de los últimos 10 archivos que han sido editados.

Con el menú *Configuración* se activa el Panel de control y la administración de impresoras.

Con el menú *Buscar* podrá buscar un archivo, una carpeta o un ordenador en la red.

El menú *Ayuda* ofrece un resumen de las funciones más importantes del entorno de Windows NT 4.0.

Existe un comando *Ejecutar*, con el cual se pueden iniciar programas desde el disco duro o desde la unidad de disquete indicando o seleccionando el nombre de archivo exacto y la ruta de acceso.

En el extremo derecho de la barra de tareas, Windows NT 4.0 muestra en un pequeño cuadro la hora actual. Este cuadro contiene iconos para componentes del sistema, como impresoras, modems o programas del sistema.

El administrador de Archivos de Windows 3.x también se localiza fácilmente. Tiene un aspecto distinto y ahora se denomina Explorador. Este es una ventana dividida en dos partes:

En la parte izquierda, el árbol de directorios completo con todas las unidades locales y de red disponibles.

En la parte derecha, las carpetas o archivos de la unidad o de la carpeta seleccionada.

La mejor forma de realizar operaciones con archivos, como copiar o mover, es mediante el ratón. Por ejemplo para eliminar un archivo basta con arrastrarlo hasta la Papelera de reciclaje.

Cabe destacar también la función del botón derecho del ratón, que ofrece menús contextuales con los comandos disponibles, está operativo en cualquier lugar del escritorio. Pulsando dicho botón en un lugar vacío del escritorio se pueden editar las propiedades del mismo: diseño del fondo, protector de pantalla o propiedades generales de las ventanas.

Resumiendo lo dicho hasta ahora podemos decir que el nuevo entorno de Windows esta ampliamente orientado a *objetos*.

Para finalizar el trabajo con Windows NT pulse el botón *Inicio* y elija la opción *Apagar el sistema.* Posteriormente le aparecerá el cuadro de diálogo Salir de Windows, donde podrá decidir si quiere:

Apagar el equipo.

Reiniciar el equipo.

Iniciar la sesión como un usuario distinto.

1.2 Novedades de Windows NT 4.0

Windows NT 4.0 Workstation

El nuevo entorno

Windows NT 4.0 contiene ahora el entorno de Windows 95.Con ello, no sólo adquiere un nuevo aspecto, sino que también toda la funcionalidad de ese entorno.

Internet Explorer

Windows NT se suministra ahora junto con el navegador WWW Internet Explorer.

Microsoft Exchange

Microsoft Exchange es un programa con el que se puede controlar y administrar toda la comunicación electrónica desde un solo programa de aplicación.

A diferencia de Windows 95, Exchange no dispone de controlador de fax integrado.

Perfiles de hardware

Con perfiles de hardware es posible guardar diversas configuraciones y abrirlas fácilmente mediante sus nombres.

Servicios clientes para Netware

En Windows NT Workstation, el servicio de cliente se ocupa de utilizar los recursos Netware. Con esta herramienta, es posible manejar ordenadores Windows NT en una red NetWare 3.1x/4.x y utilizar recursos compartidos en dicha red a través de Servicios de directorio Netware.

Modelo de objetos de componentes distribuidos (DCOM)

Con esta herramienta, se pueden utilizar y gestionar aplicaciones cliente/servidor distribuidas a través de la red, del mismo modo que si fueran aplicaciones locales en un ordenador.

DirectX

DirectX es un nuevo estándar de Microsoft especial para programar juegos y otras aplicaciones gráficas. Las interfaces de programación de aplicaciones DirectX (API) trabajan directamente junto con los subsistemas de gráficos y de sonido y, por lo tanto aprovechan la capacidad de los aceleradores gráficos modernos.

Servicios Web Punto a punto

Servicios Web punto a punto es un servidor WWW sencillo especialmente desarrollado para Windows NT Workstation. Su objetivo no es facilitar servicios WWW en Internet, sino intercambiar información a través de WWW en intranets basadas en TCP/IP (o sea, soluciones internas de la empresa).

Cliente de protocolo de túnel punto a punto (PPTP)

El protocolo punto a punto (PPP) se utiliza para redes TCP/IP a través de conexiones serie (teléfono analógico, RDSI). Generalmente se emplea para acceder a un servidor Windows NT o para establecer una conexión con un proveedor de servicios de Internet. Con algunos proveedores se requiere además un soporte SLIP para darse de alta. SLIP es el protocolo predecesor de PPP.

Con PPTP, Windows NT ofrece un protocolo PPP perfeccionado para una transferencia de datos segura a través de las líneas telefónicas. La versión Workstation de Windows NT 4.0 contiene el cliente para este protocolo, mientras que, como ya comentaremos más adelante, la versión para el servidor incluye el servidor PPTP.

Conexión mediante Acceso telefónico a redes

El servicio de acceso remoto (RAS) ya conocido en la versión 3.51 se presenta ahora en NT 4 como la red de acceso telefónico a redes en la carpeta *Accesorios*.

Ahora es posible iniciar la sesión en un dominio Windows NT a través de una red RAS directamente desde la consola de registro, mediante un botón de opción.

Windows NT 4.0 Server

La versión de Windows NT Server, es una ampliación exhaustiva de la versión Workstation. Es por ello que contiene todas las novedades mencionadas en el apartado anterior. Adicionalmente se han mejorado o incorporado algunos servicios de servidor especiales.

Servidor de nombres DNS

En Internet, el Sistema de nombres de dominio(DNS) coordina nombres de dirección universal única de un

ordenador. Windows NT 4.0 Server, también puede encargarse de este servicio.

Integración de WINS y DNS

Como Windows NT hasta ahora no soportaba DNS, se tuvo que construir un puente llamado WINS, un sistema de nombres propio. NT 4.0 integra DNS y WINS en un entorno gráfico.

DNS soporta UNC

En Internet existen determinadas convenciones de nombres, denominada Convención de nombres uniformes (UNC). Los servidores DNS de Windows NT soportan estas convenciones.

FrontPage versión 1.1

Con FrontPage es posible crear y administrar sitios web profesionales que pueden enviarse a Internet o a la intranet a través de Internet Information Server.

Microsoft Internet Information Server

Junto con Windows NT Server se suministra Internet Information Server, un servidor WWW, Gopher y FTP. Con él es posible ofrecer estos servicios en toda la red Internet o en una intranet. Information Server de Microsoft se puede vincular fácilmente con bases de datos controladas por Windows NT.

Encaminador de protocolos múltiples (MPR)

Con el servicio encaminador de protocolos múltiples (MPR) es posible establecer una interfaz para distintos servicios de red.

Con él es posible, por ejemplo, enviar datos desde el exterior a redes internas.

En este tipo de organización sólo un ordenador tiene una conexión directa con el exterior, y en la red sólo es necesario un protocolo.

Inicio remoto de ordenadores Windows 95

Los ordenadores Windows 95 pueden ser iniciados por NT Server. De este modo se crean, fácilmente, ordenadores cliente sin disco duro y unidades de disquete susceptibles de transmitir virus.

Administración remota

A través de los sistemas de escritorio Windows 95 y Windows NT también es posible administrar servidores a través de la red.

Agente basado en DHCP

En Internet, los protocolos BOOTP y DHCP asignan automáticamente una dirección IP a los ordenadores que no tienen una fija, cuando estos acceden a Internet. Windows NT también puede realizar ahora esta tarea y encaminar correctamente paquetes de datos a una red de este tipo con direcciones IP dinámicas.

Servicios Gateway para Netware

El servicio Gateway para Netware se ha ampliado en NT 4.0 con una nueva función: las estaciones de trabajo

que utilizan exclusivamente el software cliente de Microsoft ahora pueden darse de alta al árbol NDS de una red Netware 4.11 a través del servidor NT.

Soporte de servidor PPTP

Windows NT Server soporta el protocolo PPTP, que en comparación con PPP garantiza una gran seguridad en redes RAS. De esta forma, las redes Windows NT pueden combinarse a través de Internet con Redes virtuales personales (VPN).

Editor de directivas de sistema

Con el editor de directivas de sistema podrá controlar la configuración de ordenadores e instalar un entorno de trabajo unitario en los ordenadores cliente.

Monitor de red

Con el monitor de red puede comprobar y analizar a nivel de paquetes el flujo de datos enviados y recibidos en el servidor NT.

Asistentes de administración

Este asistente hará la vida un poco más fácil a los administradores del sistema, haciendo las tareas rutinarias. De este modo resulta muy sencillo, por ejemplo, instalar nuevos usuarios, compartir recursos o administrar licencias, impresoras o modems.

2 CARACTERISTICAS PRINCIPALES DE WINDOWS NT

A continuación se explicaran las principales características de Windows NT de forma no muy extensa (simplemente para tener una noción desde el principio), ya que posteriormente serán explicadas de manera minuciosa algunas de ellas.

Las principales directrices usadas en el desarrollo de Windows NT fueron, *fiabilidad*, *rendimiento*, *portabilidad*, *compatibilidad*, *escalabilidad* y *seguridad.*

FIABILIDAD

Está especialmente indicado para estaciones de trabajo y servidores de red, los cuales necesitan el máximo rendimiento. Esta versión de Windows NT mejora las versiones anteriores proporcionando las siguientes características en fiabilidad:

Modelo cliente−servidor interno. Windows NT es un sistema operativo de 32 bits, proporciona la seguridad de que, cuando se ejecuten las aplicaciones de usuario no lo hagan en la zona de memoria que tiene asignado el núcleo del sistema, llamado Kernel.

Modelo de memoria plana de 32 bits. Un verdadero sistema operativo de 32 bits, Windows NT proporciona un modelo de 32 bits de memoria plana, lo que permite al sistema operativo un acceso a 4 GB de memoria. Con este sistema las aplicaciones se ejecutan independientemente en su zona de memoria, impidiendo que otros programas sobrescriban accidentalmente sus zonas de memoria, que es la causa más común de las caídas de los sistemas.

Modelo multitarea . Windows NT utiliza la multitarea preferente para garantizar que todas las aplicaciones que se están ejecutando pueden ejecutar los recursos de la CPU en todo momento. Es decir, evita que algunas aplicaciones monopolicen el uso de la CPU o paren totalmente el sistema por la ejecución de aplicaciones erróneas.

Sistema de ficheros transnacional (NTFS). El sistema de archivos NTFS de Windows NT es un sistema de ficheros avanzado y robusto que proporciona una mayor fiabilidad.

RENDIMIENTO

Windows NT fue también diseñado para ser un sistema operativo de alto rendimiento.

Características que contribuyen a esto son:

Diseño real en 32 bits. Todo el código de Windows NT está escrito en 32 bits, lo que le proporciona mucha más velocidad que los sistemas operativos escritos con tecnología de 16 bits.

Características de multitarea y multiproceso. Windows NT proporciona multitarea preferente, lo que permite una ejecución simultánea de todos los procesos, además soporta varias CPU lo que eleva su rendimiento.

Soporte de CPU RISC. Windows NT fue diseñado a independencia del hardware, no sólo soporta CPU basadas en INTEL, sino que soporta diferentes tipos de CPU como Poder PC, DEC Palpa y MIS.

PORTABILIDAD

En el pasado los sistemas operativos eran diseñados para plataformas hardware propias, como por ejemplo la familia Intel x86. Desgraciadamente esto impedía a los sistemas operativos ser capaces de aprovechar las ventajas de nuevos chips.

Portabilidad en Windows NT significa que este sistema operativo puede utilizarse con diferentes tipos de hardware sin necesidad de reescribir el código completamente de nuevo. Windows NT proporciona las siguientes características en portabilidad:

Arquitectura de micro−Kernel modular. Windows NT posee un diseño modular lo que le proporciona independencia del hardware. El único código específico del hardware reside en el HAL (Hardware Abstraction Layer), que consta de una pequeña porción de todo el sistema operativo. El HAL opera a bajo nivel traduciendo las operaciones de bajo nivel del sistema operativo a funciones que pueden ser entendidas por el hardware específico que se está utilizando.

Sistemas de archivos configurables. Otra de las características de Windows NT que aumenta sus posibilidades de portabilidad es su capacidad de soportar diferentes sistemas de archivos. Actualmente soporta FAT usado en sistemas DOS, HPFS usado en sistemas OS/2, NTFS sistema de archivos de NT, CDFS sistema de archivo de CD−ROM y sistemas de archivos de Macintosh. Puesto que Windows NT es un sistema modular, se le podría añadir en el futuro, de manera muy sencilla, soporte para sistemas de archivo adicionales.

COMPATIBILIDAD

Un elemento clave para la aceptación de un sistema operativo, es la capacidad de trabajar con las aplicaciones ya existentes. Windows NT es capaz de ejecutar una amplia variedad de diferentes aplicaciones e interactuar

con diferentes sistemas operativos.

Diseño de aplicaciones como subsistemas. Windows NT soporta aplicaciones MS−DOS, Windows 3.x (16 bits), Windows 95, Windows 98, POSIX y OS/2 1.x. Otra vez el diseño modular de Windows NT lo hace posible.

Subsistema Windows−On−Windows (WOW). WOW proporciona una compatibilidad excelente con Win 16, emulando por completo el entorno de Windows 3.1 y ofrece la elección de ejecutar aplicaciones Windows 3.x en un espacio de memoria compartido o separado.

Interfaz explorador de Windows 95. Se ha mantenido el interfaz gráfico de Windows 95, es realmente una copia exacta ano ser por algunas carpetas que faltan y otras que se han añadido. De hecho cuando un usuario migra de Windows 95 a Windows NT puede optar por mantener el escritorio original.

Interoperatividad con Netware. El soporte de Windows NT incluye de origen el protocolo IPX/SPX para clientes Netware 3.x y 4.x. También ofrece la capacidad de compartir archivos Netware y recursos de impresión a clientes no Netware. Windows NT Server puede importar cuantas de usuarios y los scripts de logon.

Interoperatividad con UNIX. Windows NT se comunica con sistemas Unix a través del protocolo TCP/IP. También soporta impresión TCP/IP e incluye aplicaciones de conectividad básicas como por ejemplo FTP, Telnet y Ping.

Interoperatividad con Macintosh. Windows NT ofrece un procedimiento de soporte a sistemas Apple Macintosh sin precedentes. Tanto la versión Workstation como la de Servidor soporta Appletalk, protocolo usado en las redes Macintosh. Windows NT Server permite la creación de nombres Macintosh en NTFS.

ESCALABILIDAD

Otro aspecto importante de Windows NT es que es un sistema operativo escalable. Esto quiere decir que puede ser usado por un amplio abanico de sistemas, desde un ordenador personal hasta grandes sistemas con múltiples procesadores. Una pequeña lista de las características de escalabilidad son estas:

Soporte multiplataforma. Debido a que la arquitectura del micro−Kernel está en capas y usa la capa de abstracción de hardware (HAL), Windows NT es capaz de soportar los más potentes procesadores desarrollados en el futuro.

Soporte multiprocesador. Soporta múltiples CPU, lo que le proporciona un funcionamiento más eficiente a medida que se aumentan los procesadores.

SEGURIDAD

Desde las primeras implementaciones de Windows NT se ha prestado especial atención a este apartado, para que este sistema operativo ofrezca seguridad en la protección de datos tanto a empresas como a estamentos estatales.

Windows NT tiene las siguientes características generales en cuanto a seguridad:

Soporte de seguridad de dominio. El modelo de seguridad de dominio es un sofisticado sistema de acceso a la red, de manera que se controla perfectamente los recursos de red que un usuario puede utilizar. Unos servidores especiales llamados controladores de dominio son los encargados de realizar todo el trabajo de autentificación de usuarios. La información de seguridad se guarda en una base de datos llamada SAM

(Security Account Manager) .

Sistema de archivos NTFS. Es un sistema de archivos propio de Windows NT, que complementa la seguridad del sistema. Permite a los administradores de la red el control de utilizar una variedad de acceso a la red para grupos o usuarios.

Características de tolerancia a fallos. Tolerancia a fallos significa la capacidad de un sistema para soportar los diferentes errores que se puedan producir durante su funcionamiento. La primera característica importante es el soporte RAID (Redundant Array Of Inexpensive Disk), la cual usa una tecnología parecida al disk mirroring. Si se produce un fallo en el disco, gracias al RAID la información se puede obtener de nuevo.

Otra característica importante de tolerancia a fallos es el soporte de UPS, unidades de alimentación interrumpida. Windows NT detectaría una caída de tensión en la red y conmutaría inmediatamente a la UPS.

Certificación C2 estatal. Windows NT ha obtenido la certificación C2 del gobierno de EEUU.

Entrada al sistema con Ctrl+Alt+Del. Como es conocido por todos la secuencia de estas tres teclas en muchos sistemas produce un *reboot* del sistema y su consecuente parada y pérdida de datos. Por el contrario en Windows NT esta secuencia de teclas produce la entrada al sistema.

CARACTERISTICAS ADICIONALES

Soporte para las nuevas plataformas PowerPC.

Compresión de directorios y ficheros. Esta compresión mejora la utilización del disco duro.

Compresión de Servicio de Acceso Remoto (RAS). Se ha implementado una compresión software entre WTG y Windows NT Server. Como resultado se obtiene unos mejores ratios de transferencia.

Nuevos soportes de dispositivos. Windows NT incluye en su CD−ROM de instalación soporte para más de 2.000 dispositivos diferentes.

Mejora del rendimiento. Se ha conseguido en el servidor de ficheros un rendimiento del 200 % superior a la antigua versión, utilizando de 4 a 6 megabytes menos de memoria.

Herramientas de migración a Netware. Windows NT incluye herramientas de migración a Netware pudiendo copiar cuentas de usuarios y ficheros de servidores Netware a servidores NT.

3 INSTALACIÓN DE WINDOWS NT

3.1 Requisitos del sistema para NT

Windows NT 4.0 ha sido creado como un sistema operativo para ordenadores de alto rendimiento y ofrece a los usuarios profesionales un rendimiento de sistema suficiente. Por lo tanto, los requisitos de NT en cuanto al ordenador en el que se van a instalar son claramente superiores a los que precisan otros sistemas operativos como Windows 95 o DOS/Windows 3.x. A continuación describiré que configuraciones son necesarias para poder utilizar Windows NT con un rendimiento mínimo, recomendable y para aplicaciones profesionales.

Windows NT	**Windows NT Server**	**Windows NT Server**

	Workstation	**(configuración mínima)**	**(configuración recomendada)**
Procesador	Intel 486 DX, mejor Pentium 90 o mejor aún; Alpha, MIPS, PowerPC	Pentium 90	Pentium PRO o Dual Pentium
Memoria RAM	A partir de 12 MB(Intel) o 16 MB (RISC)	A partir de 12 MB(Intel) o 16 MB (RISC)	64 MB o más
Memoria de duro	A partir de 117 MB (Intel) o 124 MB (RISC) mínimo temporalmente	A partir de 148 MB (Intel) o 158 MB (RISC) temporalmente 50 MB 50 MB	Dos discos duros disco espejo de 4 GB reflejados
Controlador	E−IDE o SCSI	E−IDE o SCSI	SCSI
Tarjeta gráfica	Tarjeta aceleradora VGA con al menos 2 MB de memoria	Sólo administración del sistema en el servidor: tarjeta S−VGA básica, si no superior	Sólo administración del sistema en el servidor: tarjeta S−VGA básica, si no superior
Unidad de CD	ATAPI, mejor SCSI	ATAPI, mejor SCSI	ATAPI, mejor SCSI

3.2 Organización de los sistemas operativos

Es posible que se quiera trabajar con más de un sistema operativo sin tener que disponer de un ordenador para cada uno de los sistemas. En este caso, es preciso llegar a una solución de compromiso e instalar en un solo ordenador varios sistemas operativos que se puedan activar durante el inicio a través de un administrador de inicio.

Si se desea montar un ordenador con distintos sistemas operativos, vale la pena planificar bien la partición adecuada para el disco duro. Algunos sistemas operativos requieren una partición primaria para su inicio; otros, tienen bastante con una partición extendida. Finalmente, las particiones pueden recibir formato de diversos sistemas de archivos, los cuales dificultan un intercambio de datos mutuo.

Estos sistemas operativos se pueden instalar de forma paralela:

Windows NT 4(versión Workstation o Server) y versiones anteriores de NT.

DOS.

Windows 95.

NeXT.

Unixware.

Netware.

OS/2.

Linux.

Los administradores de inicio de que disponen son:

Administrador de inicio de NT.

Administrador de inicio de OS/2

Administrador de inicio como LILO de Linux

Además, es posible utilizar la configuración de inicio dual de Windows 95.

En primer lugar, debería planificar, qué sistema de archivos quiere asignar a cada partición de su disco duro (ver capitulo 5). Cuando existen varias particiones primarias sólo se puede acceder a los datos de la partición activa. Por lo tanto primarias solamente deben contener los elementos esenciales del sistema operativo correspondiente. El resto de los datos están mejor guardados en unidades lógicas. Una vez se haya decidido por una combinación se sistemas de archivos, el segundo paso consiste en seleccionar el administrador de inicio adecuado.

Con Windows NT puede conmutar entre varias versiones de NT y una versión de DOS o de Windows 95. Por consiguiente si sólo deben estar instalados en su ordenador estos sistemas operativos no necesitará ningún administrador de inicio aparte.

Si, junto con Windows NT, debe utilizarse otro sistema operativo que requiera una partición primaria propia (OS/2 o Linux), es mejor emplear el administrador de inicio de OS/2 o productos adicionales (como el administrador de inicio LILO). En estos casos, será precisa una partición primaria propia en el primer disco duro (C:).

3.3 Preparación de la instalación.

Windows NT 4.0 se suministra en un CD o en un CD y tres disquetes. En la versión que sólo incluye el CD, estos tres disquetes se crean, opcionalmente, con el programa de instalación. Con dichos disquetes se llevan a cabo los primeros pasos de la instalación y se ejecuta Windows NT. A continuación se trasladan todos los archivos de sistema desde el CD o desde una unidad de disco duro temporal en la que se han copiado previamente los datos.

La opción que decida dependerá de si Windows NT 4.0 detecta directamente la unidad de CD−ROM de su ordenador o no.

Para instalar Windows NT 4.0 en un ordenador Intel, utilice el programa WINNT.EXE que se encuentra en el directorio *\i386* de CD de instalación.

Puede activar dicho programa

en Windows NT para actualizar una versión ya existente del programa, o

desde el símbolo de sistema de DOS.

En ambos casos se crearán los tres disquetes de inicio y, eventualmente, se copiaran los archivos en un directorio temporal del disco duro. Con el comandoWINNT.EXE/B es posible instalar directamente Windows NT desde la unidad de CD−ROM sin los disquetes de inicio.

Si se instala Windows NT en un ordenador sin sistema operativo, es mejor crear los disquetes de inicio en otro ordenador. Una vez iniciada la instalación, Windows NT tratará de detectar la unidad de CD−ROM y ejecutar la instalación. Si durante la instalación desde los disquetes de inicio no se detectara dicha unidad, sería preciso instalar Windows NT a través de una red o bien crear una partición DOS en el ordenador e instalar el controlador de CD−ROM. Luego se inicia el ordenador y se inicia la instalación. Dependiendo de si desea instalar Windows NT desde el CD−ROM, desde un directorio temporal o de si sólo quiere crear los disquetes

de inicio, deberá activar el programa de instalación WINNT.EXE con distintos parámetros.

La siguiente tabla ofrece un resumen de ellos.

Parámetro	**Efecto**
/S[:] Nombre de la ruta	Indica la ruta de origen de los archivos de Windows NT; también puede tratarse de una unidad de red.
/T[:] Nombre del directorio	Indica el directorio temporal en el que se guardan archivos para la instalación; también puede tratarse de una unidad de red.
/I[:] Archivo Inf	Indica el nombre del archivo de información de instalación. La opción predeterminada es el archivo DOSNET.INF.
/O	Sólo crea los disquetes de inicio.
/OX	Crea los disquetes de inicio para una instalación desde el CD−ROM (o desde disquetes).
/X	Ejecuta el programa de instalación sin disquetes de inicio.
/F	Desactiva la comprobación de los archivos para la copia en disquetes de inicio.
/C	Pasa por alto los controles de espacio disponible en los disquetes de inicio.
/B	Instalación sin disquetes; en este caso es necesario indicar mediante los datos de los archivos de instalación.
/U	Permite una instalación automática si se indica mediante la ruta de origen de los archivos de instalación.

3.4 Detección del hardware.

Cada vez más, los sistemas operativos van equipados con una detección de hardware que reconoce e instala por su cuenta cada uno de los elementos del ordenador y dispositivos periféricos. En sistemas operativos como Windows NT, Windows 95 u OS/2, es imposible que se realizan errores graves en las indicaciones y se provoquen daños en el hardware.

La instalación de un dispositivo resulta particularmente fácil si el sistema operativo suministra e instala todos los controladores necesarios. Para describir esta característica se creó la expresión Plug&Play (que traducido sería algo así como conectar y funcionar). Lamentablemente, aun no funciona de forma totalmente satisfactoria con Windows NT.

Windows NT soporta durante la instalación la característica Plug&Play para muchos dispositivos, desde tarjetas gráficas pasando por unidades de CD−ROM hasta unidades de cinta para copias de seguridad.

3.5 Instalación

Mostraremos el proceso de instalación después de crear los disquetes de inicio.

En cualquier momento de la instalación puede solicitar ayuda con la tecla <F1>.

El programa de instalación presenta un mensaje de bienvenida y pregunta si se desea instalar Windows NT ahora, reanudar una instalación interrumpida o cancelar el trabajo.

Si instala Windows NT en el ordenador por primera vez, basta con que pulse la tecla <Enter>.

Configuración de unidades de almacenamiento.

El primer paso de la instalación consiste en que Windows NT detecte las unidades de almacenamiento (CD−ROM, unidades de copia de seguridad, adaptadores SCSI) del ordenador.

Es posible instalar posteriormente unidades de almacenamiento si no han sido detectadas automáticamente. Los discos duros IDE y EIDE se detectan automáticamente en la posterior instalación de Windows NT (basta con activar el administrador de discos duros y registrar y dar formato al o a los discos en NT). Pero los discos SCSI deben ser instalados manualmente con el icono SCSI en el Panel de control de Windows NT.

El programa de instalación le muestra finalmente la configuración de las unidades de almacenamiento de todos los dispositivos detectados.

La instalación de Windows NT realiza entonces particiones, si fuera necesario, en los discos duros. Dichas particiones reciben formato con el sistema de archivos que haya indicado.

Selección del directorio raíz de Windows NT

Una vez los discos duros tengan particiones y formato, se debe indicar un directorio raíz para los archivos de sistema de Windows NT. Si anteriormente no había instalado en el ordenador ninguno de los sistemas operativos Windows NT, Windows 95, Windows 98 o Windows para trabajo en grupo, puede elegir el directorio libremente, darle un nombre y establecer la partición de destino en el disco duro.

Sin embargo, si ya había instalado alguno de los sistemas operativos anteriormente mencionados, puede sobrescribir el existente con Windows NT o bien instalar Windows NT en otro directorio (a través de la instalación personalizada).

Si elige la primera opción, las aplicaciones existentes se instalaran rápidamente si son compatibles con Windows NT, y las configuraciones personales que haya realizado se incorporaran a Windows NT. En cambio si instala el nuevo sistema operativo en otro directorio se conserva el anterior y, al iniciar, podrá elegir entre ambos sistemas con el administrador de inicio de Windows NT.

Sugerencia

En ocasiones puede ser conveniente instalar dos veces NT 4 en el disco duro. Cuando, por ejemplo, en una versión de NT debe iniciar demasiados servicios, que quizás sean incompatibles entre sí, la velocidad de ejecución de NT en parte se reduce drásticamente.

De este modo concluyen las configuraciones de instalación basadas en DOS y el programa de instalación intentará reiniciar su equipo. Para ello deberá retirar el disquete de inicio de su unidad. Por último, se cargará automáticamente el asistente de instalación, el cual le indicará los pasos necesarios.

Selección del tipo de instalación.

En el primer paso del asistente de instalación puede elegir que tipo de instalación desea ejecutar:

Instalación típica: es el tipo más sencillo. El asistente de instalación se encarga de tomar la mayoría de decisiones instalando todas las opciones predeterminadas. Windows NT se instala con todos los componentes adicionales (como HyperTerminal y MS Exchange).

Instalación portátil: esta opción se ha incorporado especialmente para la instalación de Windows NT en ordenadores portátiles. Sólo se instala una versión reducida.

Compacta: aquí sólo se instalan los archivos de sistema más importantes de Windows NT, a fin de ahorrar espacio en el disco duro.

Personalizada: con esta variante puede confirmar y modificar todas las configuraciones de la instalación. También deberá elegir los componentes del sistema que desea instalar.

Modos de licencia e introducción de los datos personales

En esta parte de la instalación debe introducir sus datos personales y un nombre para el ordenador, así como elegir el modo de licencia. Son necesarias las siguientes configuraciones:

Un nombre de usuario y una empresa a través de los cuales Windows NT le pueda identificar. Sin estos datos no puede proseguir con la instalación.

Como modo de licencia se elige entre *Por puesto* o *Por servidor.*

Información

Si elige la opción Por puesto, no podrá cambiarla posteriormente. En cambio, si elige la licencia por servidor, luego podrá cambiarla por licencia por puesto.

Indique el nombre con el que se da de alta el ordenador en la red. Este nombre no puede coincidir con el de ningún otro ordenador de la red, con el nombre del dominio ni con ningún nombre de usuario. Los nombres de los ordenadores en Windows NT pueden tener hasta 15 caracteres de longitud y no pueden contener ningún carácter especial ni acentos. El nombre de un ordenador se puede modificar en cualquier momento desde el Panel de control.

En la instalación personalizada se preguntarán los componentes que deben instalarse, impresoras locales incluidas.

Selección del tipo de servidor (sólo Windows NT Server)

Los dominios de Windows NT son administrados por un controlador principal de dominio, el cual gestiona la base de datos de seguridad con todos los datos de los usuarios. Cada dominio de Windows NT debe tener exactamente un controlador principal de dominio y uno o varios controladores de dominio de reserva (también llamados controladores de seguridad). Los controladores de dominio de reserva sólo pueden instalarse si ya funciona en la red el controlador principal de dominio.

Contraseña del administrador

El programa de instalación configura en su sistema Windows NT un acceso con el nombre de Administrador. Únicamente este usuario (siempre y cuando no asigne derechos de administrador a otros usuarios) puede realizar todas las configuraciones en el sistema local y dentro de los dominios. En este punto del programa de instalación se establece la contraseña para este acceso.

Información

Nunca olvide la contraseña del administrador. Sin este acceso después no podrá realizar ninguna modificación en el sistema.

Creación de un disquete de emergencia

Tras un bloqueo del sistema que haya dañado la totalidad de la base de datos de seguridad incluyendo las copias de seguridad, Windows NT puede restablecerse con la ayuda de un disquete. Este disquete de emergencia contiene todos los componentes del sistema que el usuario ha introducido o que Windows NT ha detectado hasta ahora.

Guarde los disquetes de emergencia en un sitio seguro

Con los disquetes de emergencia también es posible robar y falsificar ordenadores NT. Guárdelos en un lugar seguro.

3.6 Instalación en red de Windows NT

Windows NT se utiliza, en la mayoría de aplicaciones, dentro de una red, ya sea como servidor de una red Windows NT, como estación de trabajo en una red Windows o como parte de una red heterogénea.

Con el programa de instalación también se instala la funcionalidad de red de Windows NT. Debe decidir si su ordenador estará conectado en una red local o si establecerá la conexión con esa red a través de una conexión RAS. Obviamente también se pueden elegir ambas opciones a la vez..

A continuación se detallan los pasos más importantes de la instalación en red.

Instalación de Internet Information Server

Windows NT en su versión 4.0 se suministra con Internet Information Server. Si esta conectado a Internet a través de un proveedor de Internet, puede ofrecer servicios WWW y FTP.

Windows NT Server y Windows NT Workstation utilizan distintas versiones de Internet Information Server. La versión que se suministra con Windows NT Workstation está pensada para la utilización en intranets, mientras que la versión para Windows NT Server puede funcionar como un auténtico servidor WWW y FTP en Internet.

Instalación de la tarjeta de red

La parte más importante de la instalación de una conexión en red es la instalación del adaptador de red. En el caso de una LAN, se trata de la tarjeta de red, y en el caso de una WAN suele tratarse de un módem o de una tarjeta RDSI.

El programa de instalación puede detectar automáticamente la tarjeta de red instalada en su sistema si Windows NT es compatible con el adaptador de red.

Si deja que Windows NT detecte la tarjeta de red, el programa de instalación examinará el ordenador en busca de adaptadores compatibles. En caso de utilizar más de un adaptador de red, pulse el botón *Buscar siguiente* en cuanto el programa de instalación haya encontrado un adaptador.

Instalación de los protocolos de red

Después de haber instalado el adaptador de red, deberá determinar que protocolos de red serán transmitidos a través del mismo. Windows NT establece entonces una conexión entre el protocolo y los controladores para la tarjeta correspondiente (denominada *binding* o enlace).

Windows NT es compatible con los siguientes protocolos de red:

NetBEUI: NetBEUI es el protocolo estándar en las redes Microsoft Windows en Windows NT a partir de la versión 3.1, Windows para Trabajo en grupo o Windows 95. En la mayoría de los casos se utiliza en redes pequeñas, con menos de 200 clientes. NetBEUI sólo soporta un encaminamiento simple a través de funciones de *Token Ring*.

NWLink: Este protocolo compatible con IPX/SPX y, por lo tanto, con Novell Netware, se utiliza en la mayoría de redes LAN grandes. Tiene capacidades de encaminamiento y trabaja junto con aplicaciones cliente−servidor de Netware.

TCP/IP: Es el protocolo estándar en redes de área extensa y en Internet. Como TCP/IP es compatible con todas las plataformas de sistemas es el protocolo estándar en redes heterogéneas. TCP/IP tiene plena capacidad de encaminamiento.

El programa de instalación establece los enlaces de los distintos protocolos con las tarjetas de red. Los controladores de redes RAS son tratados como tarjetas de red. En primer lugar, acepte las configuraciones predeterminadas de Windows NT. La edición de los enlaces sólo merece la pena si utiliza en su ordenador varias tarjetas de red que utilizan distintos protocolos. Si eliminamos los enlaces innecesarios, la velocidad de Windows NT se incrementará.

Selección del grupo de trabajo o dominio

Windows NT soporta vinculaciones de red a través del grupo de trabajo de una red punto a punto o del dominio de una red Windows NT.

En este punto tiene que decidir si sólo desea darse de alta en un grupo de trabajo o si el ordenador debe formar parte de una red Windows NT, en cuyo dominio tendrá que darse de alta.

El primer inicio de sesión en el sistema es el del administrador, ya que aún no se ha creado ningún usuario. Además, por lo general se deberán efectuar otras configuraciones adicionales que sólo puede llevar a cabo el administrador.

Con esto concluimos la instalación propiamente dicha, ahora lo que se podría instalar son componentes opcionales como por ejemplo el módem, un CD−ROM o una tarjeta RDSI.

4 FUNDAMENTOS DE WINDOWS NT

Windows NT no es, como Windows 95, una ampliación de las anteriores versiones de DOS y Windows, sino un sistema operativo desarrollado totalmente de nuevo. Por lo tanto, no padece por naturaleza de las peculiaridades conocidas de DOS. Para conseguirlo, se diferencia tanto de esos sistemas en sus propiedades esenciales, que merece la pena tratar con más detalle la arquitectura del sistema de Windows NT.

Windows NT Server y Windows NT Workstation en realidad persiguen unos objetivos muy distintos.

Windows NT Workstation es el sistema operativo cliente interactivo, mientras que NT Server es el sistema operativo servidor de alto rendimiento.

Los objetivos de diseño del sistema en NT Workstation son un buen comportamiento temporal al intercambiar tareas (el proceso principal disfruta de la máxima prioridad en cuanto a memoria RAM en la distribución temporal), una presentación de gráficos rápida y unas necesidades mínimas de RAM.

Los objetivos de diseño del sistema en NT Server son un buen funcionamiento de red y la utilización de toda la memoria de trabajo disponible y de la CPU para un acceso rápido a los archivos de la red (el caché de archivos tiene la máxima prioridad en lo que se refiere a la memoria RAM en la distribución temporal).

A pesar de todo, estos dos sistemas operativos sólo se diferencian en algunas entradas del registro del sistema. Si se modifican estas entradas en un ordenador Windows NT Workstation, pueden iniciarse también servicios de Windows NT Server.

4.1 Evolución de NT.

Microsoft inició el desarrollo del sistema operativo Windows NT a finales de los año 80. El director del proyecto fue David Cutler, antiguo empleado de Digital y uno de los desarrolladores de VMS, competencia de UNIX hoy algo adormecida. El objetivo era un sistema que compitiera con UNIX y Netware, y que funcionara tanto en procesadores Intel como en sistemas RISC (estaciones de trabajo).

El desarrollo de NT representó para Microsoft algunos costes. Sólo para la primera versión se invirtieron más de 150 millones de dólares. A pesar de los elevados costes de desarrollo hasta ahora Microsoft no había comercializado de forma agresiva Windows NT. La primera versión de NT, la 3.1, requería un hardware tan caro e insólito que pocos usuarios estaban dispuestos a instalar. Además, apenas había programas de aplicación que funcionaran en NT y sacaran provecho de todas las ventajas de este sistema operativo de 32 bits.

Hasta la aparición de la versión 3.5 no se detectaban discos duros (E)IDE y unidades CD−ROM. Con la versión 3.51 se agregó entre otras cosas, la compatibilidad con tarjetas PCMCIA. El descenso de los precios del hardware −y sobre todo de la memoria− incrementó el atractivo de Windows NT. Gracias al desarrollo del procesador Pentium PRO de Intel, Windows NT ha consiguió una plataforma eficaz y compite con las estaciones de trabajo UNIX.

NT se estableció en primer lugar como servidor de aplicaciones (por ejemplo para bases de datos como ORACLE, SQL, para sistemas Groupwise como Lotus Notes y últimamente como plataforma para R/3). Cada vez más NT hacía la competencia − especialmente en cuanto a la integración del sistema con la familia MS−BackOffice− a los tradicionalmente potentes servidores de aplicaciones y de archivos como Novell Netware en las versiones 3.12 y 4.1, sobretodo en nuevas instalaciones y en redes pequeñas y medianas−grandes.

En cambio OS/2 parece ir perdiendo importancia en la empresa. Actualmente, el OS/2 tiene aun una gran implantación en bancos y aseguradoras y se utiliza como servidor de aplicaciones (por ejemplo para el control del servicio de extranjero y de divisas).

En estos ámbitos se apreció mucho la cada vez mayor (hasta la versión 3.51) fiabilidad del sistema operativo NT, que reducía los trabajos de mantenimiento para servidores NT. Además, se ha hecho un favor a los administradores del sistema con el entorno de usuario totalmente gráfico, el cual facilita notablemente las tareas de administración diarias y reduce el periodo de formación.

Como estación de trabajo Windows NT se utiliza únicamente en ámbitos de altas prestaciones, como por ejemplo el software CAD profesional, debido a sus altos requerimientos de hardware. Hasta ahora, en redes, generalmente se conectaban clientes de Windows para Trabajo en grupo en 3.11 o clientes de Windows 95 con un servidor NT, ya que los ordenadores antiguos no cumplían los elevados requerimientos de hardware de una estación de trabajo Windows NT. Pero entonces no se dispone de las características de seguridad y comodidad de los entornos puramente NT.

Por lo que respecta a ofrecer servicios de Internet, las soluciones de Windows NT cada vez despiertan mayor

interés. Si bien hasta hace no mucho tiempo se encontraban casi exclusivamente servidores WWW basados en UNIX, actualmente aparecen cada vez más sitios NT en la red global de datos y más servidores Web comerciales. Esta tendencia aun se acentuará más con la versión 4.0 puesto que ahora se ha integrado Internet Information Server para construir una Internet o un acceso a Internet en el sistema operativo.

Con la versión 4.0, Windows NT gana mercado como sistema operativo de escritorio. Es por ello que en el mismo se ha incorporado el entorno de Windows 95 que ya estaba disponible como versión beta para la versión 3.51. Va especialmente dirigido a usuarios que no quieren renunciar a la comodidad de manejo del entorno de Windows, pero desean utilizar un sistema operativo seguro y con capacidades de multiusuario. Especialmente en redes grandes destaca de forma positiva un entorno de usuario sólido en clientes y servidores. Hasta el año 1997 se calcula en este ámbito cuotas de mercado de más del 20 % para NT, más del 40 % para Windows 95 y claramente menos del 10% para OS/2.

4.2 Estructura del sistema operativo

En este apartado presentaré el modo en el que trabaja Windows NT 4.0 tras su nuevo entorno.

4.2.1 Arquitectura

Comprender cómo funciona Windows NT es fundamental para programar y recomendable para administrarlo. Vamos a hacer un recorrido por las profundidades de este sistema operativo.

4.2.1.1 Introducción

Windows NT presenta una arquitectura del tipo cliente−servidor. Los programas de aplicación son contemplados por el sistema operativo como si fueran clientes a los que hay que servir, y para lo cual viene equipado con distintas entidades servidoras.

Uno de los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo Kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro−kernel.

Por tanto en un primer acercamiento a la arquitectura distinguimos un núcleo que se ejecuta en modo privilegiado, y se denomina Executive, y unos módulos que se ejecutan en modo no privilegiado, llamados subsistemas protegidos.

Los programas de usuario (también llamados programas de aplicación) interaccionan con cualquier sistema operativo (S.O. en adelante) a través de un juego de llamadas al sistema propio de dicho sistema. En el mundo Windows en general, las llamadas al sistema se denominan API (Application Programming Interfaces, interfaces para la programación de aplicaciones). En Windows NT y en Windows 95 se usa una versión del API llamada API Win32.

4.2.1.2 Los subsistemas protegidos.

Son una serie de procesos servidores que se ejecutan en modo no privilegiado, al igual que los procesos de usuario, pero que tienen algunas características propias que los hacen distintos.

Se inician al arrancar el S.O. y existen dos tipos: integrales y de entorno.

Un subsistema integral es aquel servidor que ejecuta una función crítica del S.O. (como por ejemplo el que gestiona la seguridad). Un subsistema de entorno da soporte a aplicaciones procedentes de S.O. distintos, adaptándolas para su ejecución bajo Windows NT. Existen tres de este tipo:

Win32, que es el principal, y proporciona la interfaz para aplicaciones específicamente construidas para Windows NT.

POSIX, que soporta aplicaciones UNIX.

OS/2, que da el entorno a aplicaciones procedentes del S.O. del mismo nombre.

El subsistema Win32.

Es el más importante, ya que atiende no sólo a las aplicaciones nativas de Windows NT, sino que para aquellos programas no Win32, reconoce su tipo y los lanza hacia el subsistema correspondiente. En el caso de que la aplicación sea MS−DOS o Windows de 16 bits (Windows 3.11 e inferiores), lo que hace es crear un nuevo subsistema protegido. Así, la aplicación DOS o Win16 se ejecutaría en el contexto de un proceso llamado VDM (Virtual DOS Machine, máquina virtual DOS), que no es más que un simulador de un ordenador funcionando bajo MS−DOS. Las llamadas al API Win16 serían correspondidas con las homónimas en API Win32. Microsoft llama a esto WOW (Windows On Win32). El subsistema soporta una buena parte del API Win32. Así, se encarga de todo lo relacionado con la interfaz gráfica con el usuario (GUI), controlando las entradas del usuario y salidas de la aplicación. Por ejemplo, un buen número de funciones de las bibliotecas USER32 y GDI32 son atendidas por Win32, ayudándose del Executive cuando es necesario. El funcionamiento como servidor de Win32 lo veremos un poco más adelante, en el apartado de llamadas a procedimientos locales.

El subsistema POSIX.

La norma POSIX (Portable Operating System Interface for UNIX) fue elaborada por IEEE para conseguir la portabilidad de las aplicaciones entre distintos entornos UNIX. La norma se ha implementado no sólo en muchas versiones de UNIX, sino también en otros S.O. como Windows NT, VMS, etc. Se trata de un conjunto de 23 normas, identificadas como IEEE 1003.0 a IEEE 1003.22, o también POSIX.0 a POSIX.22, de las cuales el subsistema POSIX soporta la POSIX.1, que define un conjunto de llamadas al sistema en lenguaje C. El subsistema sirve las llamadas interaccionando con el Executive. Se encarga también de definir aspectos específicos del S.O. UNIX, como pueden ser las relaciones jerárquicas entre procesos padres e hijos (las cuales no existen en el subsistema Win32, por ejemplo, y que por consiguiente no aparecen implementadas directamente en el Executive).

El subsistema OS/2.

Igual que el subsistema POSIX proporciona un entorno para aplicaciones UNIX, este subsistema da soporte a las aplicaciones del S.O. OS/2. Proporciona la interfaz gráfica y las llamadas al sistema; las llamadas son servidas con ayuda del Executive.

En cuanto a los subsistemas integrales, destacamos dos:

El subsistema proceso de inicio.

El proceso de inicio (Logon Process) recibe las peticiones de conexión por parte de los usuarios. En realidad son dos procesos, cada uno encargándose de un tipo distinto de conexión: el proceso de inicio local, que gestiona la conexión de usuarios locales directamente a una máquina Windows NT; y el proceso de inicio remoto, el cual gestiona la conexión de usuarios remotos a procesos servidores de NT.

El subsistema de seguridad.

Este subsistema interacciona con el proceso de inicio y el llamado monitor de referencias de seguridad (del que trataremos en el Executive), de esta forma se construye el modelo de seguridad en Windows NT. El subsistema de seguridad interacciona con el proceso de inicio, atendiendo las peticiones de acceso al sistema. Consta de dos subcomponentes: la autoridad de seguridad local y el administrador de cuentas.

El primero es el corazón del subsistema de seguridad, en general gestiona la política de seguridad local, así, se encarga de generar los permisos de acceso, de comprobar que el usuario que solicita conexión tiene acceso al sistema, de verificar todos los accesos sobre los objetos (para lo cual se ayuda del monitor de referencias a seguridad) y de controlar la política de auditorías, llevando la cuenta de los mensajes de auditoría generados por el monitor de referencias.

El administrador de cuentas mantiene una base de datos con las cuentas de todos los usuarios (login, claves, identificaciones, etc.). Proporciona los servicios de validación de usuarios requeridos por el subcomponente anterior.

4.2.1.3 El Executive.

No debemos confundir el Executive con el núcleo de Windows NT, aunque muchas veces se usan (incorrectamente) como sinónimos. El Executive consta de una serie de componentes software, que se ejecutan en modo privilegiado, uno de los cuales es el núcleo. Dichos componentes son totalmente independientes entre sí, y se comunican a través de interfaces bien definidas. Recordemos que en el diseño se procuró dejar el núcleo tan pequeño como fuera posible y, como veremos, la funcionalidad del núcleo es mínima.

El administrador de objetos (Object Manager).

Se encarga de crear, destruir y gestionar todos los objetos del Executive. Tenemos infinidad de objetos: procesos, subprocesos, ficheros, segmentos de memoria compartida, semáforos, mutex, sucesos, etc. Los subsistemas de entorno (Win32, OS/2 y POSIX) también tienen sus propios objetos. Por ejemplo, un objeto ventana es creado (con ayuda del administrador de objetos) y gestionado por el subsistema Win32. La razón de no incluir la gestión de ese objeto en el Executive es que una ventana sólo es innata de las aplicaciones Windows, y no de las aplicaciones UNIX o OS/2. Por tanto, el Executive no se encarga de administrar los objetos relacionados con el entorno de cada S.O. concreto, sino de los objetos comunes a los tres.

El administrador de procesos (Process Manager).

Se encarga (en colaboración con el administrador de objetos) de crear, destruir y gestionar los procesos y subprocesos. Una de sus funciones es la de repartir el tiempo de CPU entre los distintos subprocesos. Suministra sólo las relaciones más básicas entre procesos y subprocesos, dejando el resto de las interrelaciones entre ellos a cada subsistema protegido concreto. Por ejemplo, en el entorno POSIX existe una relación filial entre los procesos que no existe en Win32, de manera que se constituye una jerarquía de procesos. Como esto sólo es específico de ese subsistema, el administrador de objetos no se entromete en ese trabajo y lo deja en manos del subsistema.

El administrador de memoria virtual (Virtual Memory Manager).

Windows NT y UNIX implementan un direccionamiento lineal de 32 bits y memoria virtual paginada bajo demanda. El VMM se encarga de todo lo relacionado con la política de gestión de la memoria. Determina los conjuntos de trabajo de cada proceso, mantiene un conjunto de páginas libres, elige páginas víctima, sube y baja páginas entre la memoria RAM y el archivo de intercambio en disco, etc.

La facilidad de llamada a procedimiento local (LPC Facility).

Este módulo se encarga de recibir y enviar las llamadas a procedimiento local entre las aplicaciones cliente y los subsistemas servidores.

El administrador de entrada/salida (I/O Manager).

Consta de varios subcomponentes: el administrador del sistema de ficheros, el servidor de red, el redirector de red, los drivers de dispositivo del sistema y el administrador de cachés.

Buena parte de su trabajo es la gestión de la comunicación entre los distintos drivers de dispositivo, para lo cual implementa una interfaz bien definida que permite el tratamiento de todos los drivers de una manera homogénea, sin preocuparse del funcionamiento específico de cada uno. Trabaja en conjunción con otros componentes del Executive, sobre todo con el VMM. Le proporciona la E/S síncrona y asíncrona, la E/S a archivos asignados en memoria y las caches de los ficheros. El administrador de caches no se limita a gestionar unos cuantos buffers de tamaño fijo para cada fichero abierto, sino que es capaz de estudiar las estadísticas sobre la carga del sistema y variar dinámicamente esos tamaños de acuerdo con la carga. El VMM realiza algo parecido en su trabajo.

El monitor de referencias a seguridad.

Este componente da soporte en modo privilegiado al subsistema de seguridad, con el que interacciona. Su misión es actuar de alguna manera como supervisor de accesos, ya que comprueba si un proceso determinado tiene permisos para acceder a un objeto determinado, y monitoriza sus acciones sobre dicho objeto. De esta manera es capaz de generar los mensajes de auditorías. Soporta las validaciones de acceso que realiza el subsistema de seguridad local.

El núcleo (Kernel).

Situado en el corazón de Windows NT, se trata de un micro−kernel que se encarga de las funciones más básicas de todo el sistema operativo: ejecución de subprocesos, sincronización multiprocesador, manejo de las interrupciones hardware.

El nivel de abstracción de hardware (HAL).

Es una capa de software incluida en el Executive que sirve de interfaz entre los distintos drivers de dispositivo y el resto del sistema operativo. Con el HAL, los dispositivos se presentan al S.O. como un conjunto homogéneo con el cual interacciona a través de un conjunto de funciones bien definidas. Estas funciones son llamadas tanto desde el S.O. como desde los propios drivers. Permite a los drivers de dispositivo adaptarse a distintas arquitecturas de E/S sin tener que ser modificados en gran medida. Además oculta los detalles hardware que conlleva el multiprocesamiento simétrico de los niveles superiores del S.O.

4.2.1.4 Llamadas a procedimientos locales y remotos.

Windows NT, al tener una arquitectura cliente−servidor, implementa el mecanismo de llamada a procedimiento remoto (RPC) como medio de comunicación entre procesos clientes y servidores, situados ambos en máquinas distintas de la misma red. Para clientes y servidores dentro de la misma máquina, la RPC toma la forma de llamada a procedimiento local (LPC). Vamos a estudiar en detalle ambos mecanismos pues constituyen un aspecto fundamental del diseño de NT.

Llamada a Procedimiento Remoto (Remote Procedure Call −RPC).

Se puede decir que el sueño de los diseñadores de Windows NT es que algún día se convierta en un sistema distribuido puro, es decir, que cualquiera de sus componentes pueda residir en máquinas distintas, siendo el Kernel en cada máquina el coordinador general de mensajes entre los distintos componentes. En la última versión de Windows NT esto no es aún posible. No obstante, el mecanismo de RPC permite a un proceso cliente acceder a una función situada en el espacio virtual de direcciones de otro proceso servidor situado en otra máquina de una manera totalmente transparente. Vamos a explicar el proceso en conjunto.

Supongamos que tenemos un proceso cliente ejecutándose bajo una máquina A, y un proceso servidor bajo una máquina B. El cliente llama a una función f de una biblioteca determinada. El código de f en su biblioteca es una versión especial del código real; el código real reside en el espacio de direcciones del servidor. Esa versión especial de la función f que posee el cliente se denomina proxy. El código proxy lo único que hace es recoger los parámetros de la llamada a f, construye con ellos un mensaje, y pasa dicho mensaje al Executive. El Executive analiza el mensaje, determina que va destinado a la máquina B, y se lo envía a través del interfaz de transporte. El Executive de la máquina B recibe el mensaje, determina a qué servidor va dirigido, y llama a un código especial de dicho servidor, denominado stub, al cual le pasa el mensaje. El stub desempaqueta el mensaje y llama a la función f con los parámetros adecuados, ya en el contexto del proceso servidor. Cuando f retorna, devuelve el control al código stub, que empaqueta todos los parámetros de salida (si los hay), forma así un mensaje y se lo pasa al Executive. Ahora se repite el proceso inverso; el Executive de B envía el mensaje al Executive de A, y este reenvía el mensaje al proxy. El proxy desempaqueta el mensaje y devuelve al cliente los parámetros de retorno de f. Por tanto, para el cliente todo el mecanismo ha sido transparente. Ha hecho una llamada a f, y ha obtenido unos resultados; ni siquiera tiene que saber si el código real de f está en su biblioteca o en una máquina situada tres plantas más abajo, esta es la elegancia de las RPC.

Llamada a procedimiento local (Local Procedure Call −LPC).

Las LPC se pueden considerar una versión descafeinada de las RPC. Se usan cuando un proceso necesita los servicios de algún subsistema protegido, típicamente Win32. Vamos a intentar descubrir su funcionamiento.

El proceso cliente tiene un espacio virtual de 4 Gb. Los 2 Gb inferiores son para su uso (excepto 128 Kb). Los 2 Gb superiores son para uso del sistema. Vamos a suponer que el cliente realiza una llamada a la función CreateWindow. Dicha función crea un objeto ventana y devuelve un descriptor al mismo. No es gestionada directamente por el Executive, sino por el subsistema Win32 (con algo de colaboración por parte del Executive, por supuesto; por ejemplo, para crear el objeto). El subsistema Win32 va guardando en su propio espacio de direcciones una lista con todos los objetos ventana que le van pidiendo los procesos. Por consiguiente, los procesos no tienen acceso a la memoria donde están los objetos; simplemente obtienen un descriptor para trabajar con ellos. Cuando el cliente llama a CreateWindow, se salta al código de esa función que reside en la biblioteca USER32.DLL asignada en el espacio de direcciones del cliente. Por supuesto, ese no es el código real, sino el proxy. El proxy empaqueta los parámetros de la llamada, los coloca en una zona de memoria compartida entre el cliente y Win32, pone al cliente a dormir y ejecuta una LPC. La facilidad de llamada a procedimiento local del Executive captura esa llamada, y en el subsistema Win32 se crea un subproceso que va a atender a la petición del cliente. Ese subproceso es entonces despertado, y comienza a ejecutar el correspondiente código de stub. Los códigos de stub de los subsistemas se encuentran en los 2 Gb superiores (los reservados) del espacio virtual del proceso cliente. Aunque no he encontrado más documentación al respecto, es muy probable que dichos 2 Gb sean los mismos que se ven desde el espacio virtual de Win32. Sea como sea, el caso es que el stub correspondiente desempaqueta los parámetros del área de memoria compartida y se los pasa a la función CreateWindow situada en el espacio de Win32. Ése sí es el código real de la función. Cuando la función retorna, el stub continúa, coloca el descriptor a la ventana en la memoria compartida, y devuelve el control de la LPC al Executive. El subproceso del Win32 es puesto a dormir. El Executive despierta al subproceso cliente, que estaba ejecutando código proxy. El resto de ese código lo que hace es simplemente tomar el descriptor y devolverlo como resultado de la función CreateWindow.

Novedades de la versión 4.0

Con al versión 4.0 de Windows NT, Microsoft ha dado otro paso hacia delante en lo que se refiere a un sistema operativo puramente de micronúcleo. Dos partes esenciales del subsistema WIN32, que funcionan en modo usuario, se han trasladado al micronúcleo y funcionan en modo núcleo:

el archivo *User.exe* (administrador de ventanas) y

el archivo *Gdi.exe*(GDI, interfaz de dispositivos gráficos), el sistema de salida de gráficos de Windows NT.

Para comprender la función de estos dos archivos y la importancia de esta modificación, es necesario observar con detalle en primer lugar el subsistema WIN32, en el cual estaban integrados estos archivos hasta ahora.

El subsistema WIN32 fue pensado originalmente como unidad independiente. Todas las partes de este sistema debían estar rigurosamente separadas entre sí y debían funcionar de forma independiente del resto de áreas del sistema operativo. Este procedimiento garantiza una alta seguridad, pero resta rendimiento. Muchos elementos de cada una de las partes del subsistema WIN32 se repiten, aunque deben ser tratadas individualmente en cada parte, por lo que consumen innecesariamente espacio de disco duro.

El subsistema WIN32, hasta la versión 3.51 de Windows NT, estaba formado por los siguientes componentes:

Administrador de ventanas: control de las funciones de entrada y salida y de pantalla.

Interfaz de dispositivos gráficos: biblioteca con los elementos del entorno gráfico de usuario.

Controladores de dispositivos gráficos: controladores dependientes del hardware para el control de la tarjeta gráfica.

Consola: control de la interfaz de comandos de Windows NT.

Funciones del sistema operativo: conexión de los componentes en el subsistema WIN32.

El problema esencial de esta organización consistía en que el subsistema WIN32 contenía todas las funciones para la salida de gráficos. Durante el trabajo con un sistema operativo pueden realizarse perfectamente varios centenares de peticiones por segundo al sistema de gráficos. En el sistema WIN32 estas peticiones deben ser descompuestas en subprocesos (threads) y procesos, y la CPU debe procesarlas. Debido a la rigurosa separación de los componentes, muchos procesos se tratan doblemente. Por lo tanto, esta organización no sólo requiere espacio de memoria, sino también tiempo de la CPU.

A pesar de que la separación de los archivos *User.exe* y *Gdi.exe* del micronúcleo en Windows NT 3.51 funciona de modo muy satisfactorio, Microsoft se ha decidido por el desplazamiento al micronúcleo. Para ello era decisivo el hecho de que Windows NT fuera un sistema operativo gráfico: existen numerosas ejecuciones de las rutinas gráficas de salida y cada aplicación en Windows NT utiliza dichas rutinas. Por lo tanto si se desplazan al modo núcleo, se ejecutarán con mayor prioridad y estarán protegidas ante los accesos directos mediante programas de aplicación.

El resultado es en este caso, una mayor velocidad de procesamiento, especialmente en Windows NT Workstation y una menor carga de memoria del sistema. Naturalmente, el procedimiento también tiene inconvenientes: el micronúcleo crece de forma continua y las necesidades de memoria se desvían a otro punto. Lo problemático es que el núcleo de NT Workstation y NT Server únicamente se modifica por razones de rendimiento. La presentación acelerada de gráficos solo es conveniente para estaciones de trabajo NT; para servidores NT es innecesaria esta modificación del diseño, ya que aquí son importantes el cache de archivos y

los procesos de lectura y escritura. De todos modos, los servidores NT en las empresas funcionan de forma dedicada (no se utilizan como puestos de trabajo), de modo que nadie sacaría provecho de una presentación de gráficos acelerada. Los críticos reprochan a Microsoft que con la modificación del núcleo se ha puesto en peligro la estabilidad de los servidores NT para ganar pocas mejoras de rendimiento es la estación de trabajo NT.

La ventaja especial de la nueva organización es que los accesos al hardware de los componentes WIN32 ya no tienen lugar a través de la interfaz entre el modo usuario y el modo núcleo, sino directamente desde el modo núcleo. Esto acelera especialmente los accesos al sistema de gráficos.

Como ya sucedía en el anterior subsistema WIN32, los accesos a los archivos *Use.exe* y *Gdi.exe* se aceleran mediante procedimientos de procesamiento por lotes y de caché. Con el primer procedimiento, las peticiones se gestionan en una cola de espera. Puesto que cualquier petición tiene aquí una mayor prioridad, es posible avanzar al hardware los accesos importantes. Con el procedimiento de caché los datos se guardan provisionalmente en el disco duro, como ocurre en el acceso de lectura y escritura.

Fiabilidad

Los sistemas operativos de alto rendimiento como Windows NT viven de su fiabilidad. A menudo se emplean en aplicaciones dedicadas (como bases de datos y sistemas de registro) o en servidores y, por lo tanto, deben ser particularmente estables. Además deben proteger los datos importantes de accesos no autorizados a estos ordenadores. Para cumplir con estos requisitos se precisan determinados elementos en el sistema operativo.

Todo los procesos de un sistema operativo requieren memoria RAM auténtica o direcciones de memoria en el procesador. La mayoría de fallos de los sistemas operativos como Windows 95 o Windows para Trabajo en grupo se basan en que dos aplicaciones o procesos intentan utilizar la misma memoria, interfiriéndose mutuamente. El resultado de ello son los fallos de protección general (suficientemente conocidos).

En Windows NT, todos los procesos se desarrollan en áreas de memoria rigurosamente separadas. Además, se produce una separación entre los procesos en modo usuario y en modo núcleo:

Los procesos en modo usuario sólo pueden leer y escribir en el área de memoria que tienen asignada. No pueden utilizar la memoria de otra aplicación en modo usuario ni acceder a áreas de memoria utilizadas por los subsistemas del modo núcleo. Hasta la versión 3.51 de Windows NT esta limitación afectaba también a los archivos *Gdi.exe* y *User.exe.*

Los procesos del modo núcleo, que deben ser utilizados por todas las aplicaciones, emplean básicamente el área de memoria asignada al modo núcleo. Esta área de memoria está protegida ante accesos mediante aplicaciones y subsistemas en modo usuario. Las aplicaciones del modo núcleo también pueden acceder en determinadas situaciones al área de memoria de las aplicaciones del modo usuario y abrir subprocesos en ellas.

Para acceder a los archivos del modo núcleo, los procesos y aplicaciones del modo usuario utilizan interfaces especiales. Para el acceso a los archivos *Gdi.exe* y *User.exe* se utilizan las interfaces GDI32 y USER32 respectivamente. Estas dos interfaces ya existían en Windows NT 3.51. Protegen los archivos *Gdi.exe* y *User.exe* ante accesos mediante otras aplicaciones en modo usuario.

La organización de los importantes archivos de sistema *Gdi.exe* y *User.exe* en modo núcleo garantiza una seguridad y una estabilidad del sistema operativo máximas, puesto que estos archivos están protegidos ante accesos de la mejor forma posible. El precio que deberá pagar por ello como usuario son unos requerimientos del sistema más elevados. A pesar de que los accesos al hardware puedan acelerarse a través de la organización en modo núcleo, un modo núcleo mayor representa unos requerimientos mayores en cuanto a

procesador y memoria disponible.

Peligros de la nueva organización

Un peligro resultante de esta nueva forma de organización es que los procesos de los archivos *Gdi.exe* y *User.exe* ahora también pueden escribir en áreas de memoria de otras aplicaciones del núcleo. Por lo tanto, en principio un *Gdi.exe* bloqueado puede dejar inutilizado todo del sistema.

En la forma de organización de Windows NT 3.51, los archivos *Gdi.exe* y *User.exe* como aplicación del modo usuario no podían escribir en el modo núcleo y, por lo tanto, no influían en la estabilidad de todo el sistema.

Esto tiene consecuencias esenciales para el usuario cuya aplicación se bloquee: hasta ahora sólo se perdían los datos de la aplicación que había causado el error. Ahora se pierden los datos no guardados de todas las aplicaciones, ya que se detiene todo el sistema.

Microsoft asegura que durante lasa pruebas con Windows NT no se produjeron tales problemas.

Los controladores de las tarjetas gráficas, que hasta ahora se utilizaban en modo usuario trabajan ahora directamente en modo núcleo y, por lo tanto, pueden influir directamente en la estabilidad del todo el sistema. Aunque aquí se trata básicamente de los mismos controladores que antes, surgen peligros adicionales debido a los accesos directos al hardware de dichos controladores en modo núcleo. Dado que sólo se ha verificado la seguridad de los controladores de los componentes que figuran en la lista de compatibilidad de hardware de Microsoft, aconsejo que para un funcionamiento productivo debe elegirse únicamente un hardware como base para Windows NT.

Perspectiva

En el ámbito de los controladores de hardware se divisa una novedad decisiva: con la próxima versión de NT (5.0), Microsoft aspira a una integración del modelo común de controladores de dispositivos (CDDM) en sus sistemas operativos Windows 95 y Windows NT Workstation o Server. De esta forma es posible que los fabricantes de periféricos en el futuro tengan que suministrar un controlador común para todos los sistemas operativos de 32 bits de Microsoft (Windows 95, NT y sistemas posteriores). La consecuencia negativa, sin embargo, es que los componentes controladores existentes ya no funcionaran y tendrán que cambiarse.

Rendimiento

Microsoft no ha desplazado los archivos *Gdi.exe* y *User.exe* al modo núcleo en vano. Con el nuevo entorno de Windows 95 se ha dotado a Windows NT 4.0 de un entorno gráfico mucho más potente que en a las versiones anteriores. Lo habrá podido constatar quien haya probado la versión NT 3.51 con la interfaz de usuario gráfica de Windows 95, disponible desde fines 1995. Windows NT 3.51 era claramente más lento con el nuevo entorno.

Un efecto secundario del desplazamiento de los archivos *Gdi.exe* y *User.exe* al modo núcleo es una necesidad de memoria más reducida de esas dos aplicaciones. No obstante, el espacio ahorrado de este modo es utilizado por el explorador del entorno Windows 95, de forma que Windows NT 4.0 en total no emplea más memoria que Windows NT 3.51.

4.3 Características de rendimiento de Windows NT

En este apartado presentaré las características de rendimiento esenciales del sistema operativo multiusuario de 32 bits de Windows NT 4.0.

Multitarea y multisubproceso

Multitarea

Windows NT utiliza el método multitarea prioritario (auténtico). Con el mismo se ejecutan simultáneamente varios procesos con distintas prioridades. Así , es posible, por ejemplo, dar formato a los disquetes de inicio en el programa de instalación mientras se copian archivos temporales en el disco duro. Las tareas se distribuyen, en las unidades de control, en lapsos de tiempo.

Los conceptos multitarea sencillos utilizan el método multitarea cooperativo. Con el mismo también se asumen y gestionan varios procesos al mismo tiempo. Sin embargo, en cada momento sólo se edita un proceso, mientras que el resto se trasladan a una cola de espera.

Multisubproceso (multithreading)

El procesamiento paralelo de varias tareas en un ordenador se puede mejorar todavía. Si se realizan al mismo tiempo distintas tareas en un programa de aplicación, de poco sirve el método multitarea por si sólo. Para el procesador estas tareas son una sola, por lo que solamente se ejecutarán una tras otra.

El remedio a este problema es el multisubproceso. Con el mismo, el programa de aplicación diferencia distintas tareas mediante los denominados subprocesos. El número de subprocesos que puede administrar al mismo tiempo una aplicación depende de los recursos del sistema operativo y del software de la aplicación. Algunos programas gestionan hasta 17 subprocesos.

Un ejemplo:

Un buen ejemplo de multisubproceso es el trabajo con el navegador WWW Netscape. Con un único navegador es posible descargar archivos mediante FTP y al mismo tiempo pasar a la página WWW siguiente. Allí, se puede iniciar otra sesión FTP y asignar un tercer subproceso.

Estabilidad y seguridad

Junto con el rendimiento las características de calidad esenciales de un sistema operativo son la estabilidad y seguridad.

Windows NT ejecuta cada aplicación en un área de memoria distinta. Durante el funcionamiento normal no pueden interferir en territorio ajeno. Una aplicación que haya dejado de responder puede ser terminada (o finalizada) con el administrador de tareas, sin que el resto de aplicaciones o el propio sistema operativo finalicen.

Aunque se ejecuten aplicaciones en distintas áreas de memoria pueden producirse fallos en el sistema. Por ejemplo, si dos programas acceden al mismo tiempo al archivo de sistema *User.exe,* pueden interferirse mutuamente provocando una pérdida de datos y dejar inutilizable el archivo de sistema para cualquier otro uso posterior.

En estas situaciones Windows NT también ofrece soluciones. El servidor del sistema, responsable de las tareas fundamentales del sistema operativo, se ejecuta en un área de memoria que no puede ser utilizada por ninguna otra aplicación. Incluso si se hubiera dañado el propio entorno (*shell*) de Windows NT (el archivo *Explorer.exe*) mediante el bloqueo de otras aplicaciones, el servidor del sistema puede activar el Explorador y hacer funcionar el sistema. De este modo, un servidor Windows NT nunca puede bloquearse (por lo menos teóricamente).

Inconveniente

Naturalmente, la gestión separada de programas en áreas de memoria propias requiere unos recursos del sistema mayores que para dividir la memoria. Cada aplicación de Windows NT toma como mínimo 3 MB de memoria RAM. Si se ejecutan algunos servicios estándar o incluso de servidor en segundo plano, la memoria RAM se consume rápidamente.

Administración central

La gestión central de datos de configuración también contribuye a la seguridad y a la estabilidad de un sistema operativo. Windows NT utiliza una base de datos de configuración central, la base de datos del registro. Los antiguos usuarios de Windows 3.x se alegrarán de no tener que volver a editar un WIN.INI, un SYSTEM.INI, un AUTOEXEC.BAT, un CONFIG.SYS, etc.

Para ello es necesario trabajar con cuidado con la complicada base de datos del registro. Si se realizan configuraciones incorrectas se puede bloquear el sistema. Aunque en este caso no está todo perdido: al volver a iniciar Windows NT basta con recurrir a la última configuración buena conocida, guardada en el sistema como copia de seguridad, e intentarlo de nuevo.

Sin embargo, no confíe demasiado en estos mecanismos de rescate. Si ha efectuado modificaciones en un servicio que ha provocado el fallo del sistema y dicho servicio no se puede iniciar automáticamente, tal vez esas modificaciones surtan efecto después de varios reinicios. No obstante, si también se ha dañado la versión anterior de la base de datos de registro, no podrá trabajar más con Windows NT. Sólo le quedan los disquetes de emergencia o deberá volver a instalar el sistema de nuevo.

En el primer caso, se pierden todas las configuraciones realizadas desde la creación de los disquetes de emergencia, mientras que en el segundo caso se deben introducir de nuevo todos los datos del usuario y volver a compartir los recursos de la red si se trata de un equipo Windows NT Server.

Administración de usuarios

En una red trabajan varias personas que comparten recursos como el espacio de disco duro, el rendimiento del ordenador, la impresora y los programas de aplicación. Es evidente que, en una red de este tipo, no todo el mundo puede hacerlo todo. Para controlarlo, Windows NT soporta:

Cuentas de usuario, que establecen exactamente quien puede acceder a que recursos y de que forma.

Registros de usuarios, con los cuales se comprueba quien ha utilizado que recursos y cuando.

Registros de sucesos generales, que ayudan a encontrar el error si se produjera un fallo.

Como sistema operativo verdaderamente multiusuario, Windows NT ofrece esta administración de usuarios para todos los usuarios locales. Por lo tanto para cada usuario que se siente delante de un ordenador Windows NT puede establecer los derechos de acceso y perfiles de usuario.

Conexión con Internet

Desde el boom de Internet de 1994 y1995 la conexión de servidor a esta red mundial de datos es cada vez más importante. Con el protocolo TCP/IP los requerimientos para participar en Internet son cada vez menores, aunque con un sistema operativo para servidor como Windows NT se consigue más. También debe poder ofrecer servicios en Internet (por ejemplo un servidor WWW, telnet, un servidor FTP). Windows NT dispone de todos estos servicios.

Más adelante describiré la utilización de Windows NT (Workstation y Server) como servidor WWW.

Administración de discos duros y de archivos

Este tema será tratado con detenimiento en los temas posteriores, aquí sólo lo nombro para que quede constancia de que forma parte de las características de rendimiento de NT.

5 ADMINISTRACION DE ARCHIVOS EN NT

Los discos duros contienen el bien más preciado: los datos. Si los datos no se guardan periódicamente, la perdida de datos puede ser catastrófica para la empresa.

Existen varias posibilidades para protegerse de incidentes y sus consecuencias. El riesgo de pérdida de datos se reduce a través de:

La selección de discos duros de mayor calidad.

La elección de un sistema de archivos estable (es NT: NTFS).

La organización de datos segura y compatible con el sistema de archivos o el controlador de disco duro.

La copia de los datos realizando copias de seguridad regulares (mejor diarias) y reflejando el disco duro o utilizando sistemas RAID 5.

En este capitulo presentaré distintas posibilidades para proteger la seguridad de los datos.

Sistemas de archivos

Los sistemas de archivos organizan los datos en los discos duros distribuyéndolos en áreas físicamente accesibles del disco. Algunos sistemas de archivos aceleran los procesos de lectura y escritura con memorias caché propias.

Los sistemas operativos de ordenadores utilizan principalmente los siguientes sistemas de archivos:

FAT

HPFS

NTFS

Sistemas de archivos de los dialectos UNIX

Estos sistemas de archivos se diferencian por su seguridad y rendimiento:

FAT

Tabla de asignación de archivos (FAT) es el sistema de archivos más sencillo.

En un archivo aparte (FAT), consta en qué sectores del disco duro (o del disquete) se encuentra cada parte de un archivo. Para ello, FAT divide el disco duro en bloques. El número de bloques es limitado y todos los

bloques de un disco duro deben tener siempre el mismo tamaño. En discos duros grandes con sólo una partición FAT se pierde mucho espacio. Además, los bloques FAT grandes provocan errores de disco duro con facilidad. Los sistemas de archivos FAT hasta ahora imponían al usuario la limitación 8+3 para el nombre de archivos y directorios.

Desde la aparición de Windows 95 con su sistema de archivos FAT ampliado (V−FAT), esta limitación ya no existe. Sin embargo, V−FAT no ha podido mejorar la seguridad y la estabilidad del sistema de archivos.

Además, pronto se produce una fragmentación del disco duro, ya que la información se escribe en los bloques FAT de todo el disco.

HPFS

Sistemas de archivos de alto rendimiento (HPFS) pertenece a los sistemas de archivos instalables (IFS). Se encuentra principalmente en ordenadores OS/2, aunque originalmente fue desarrollado por Microsoft. Los sistemas de archivos HPFS son mucho más seguros, estables y rápidos que los sistemas FAT. HPFS accede a los datos del disco duro a través de un búfer de alta velocidad (cache) y soporta varias particiones activas al mismo tiempo. En los sistemas de archivos HPFS, los nombres de archivo pueden tener hasta 254 caracteres de longitud.

NTFS

El sistema de archivos de NT (NTFS) ha sido desarrollado especialmente para Windows NT. NTFS es aun más seguro y estable que HPFS, aunque necesita algo más de tiempo para acceder a los archivos. Si desea crear discos duros espejo o dividirlos en bandas con paridad, deberá utilizar una partición NTFS. Estas funciones especiales del Administrador de discos de Windows NT no son compatibles con otros sistemas de archivos.

Windows NT ofrece, junto con el sistema de archivos NTFS, medidas de seguridad ampliadas para el acceso a archivos y directorios. De forma similar a los sistemas de archivos UNIX, se pueden definir derechos sobre archivos y directorios de forma individual para cada grupo. Windows NT no ofrece ningún mecanismo de seguridad en el sistema de archivos FAT.

Así organiza NTFS los archivos.

El sistema de archivos de Windows NT considera cada sector del soporte de datos como archivo o parte de un archivo al que se le asignan determinados atributos y derechos de usuario. De modo similar a los sistemas de archivos FAT, en un archivo especial se define que sectores pertenecen a cada archivo y donde se encuentran los mismos. NTFS denomina a ese archivo MFT (Tabla maestra de archivos). La MFT también contiene una entrada de registro, que se encarga de restablecer archivos en Windows NT. En la MFT se comparte para cada archivo un determinado espacio, que luego puede incorporar la información sobre donde está guardado del archivo.

Los archivos pequeños también pueden incorporarse directamente en este espacio, mientras que los archivos grandes se guardan en forma de un Btree. NT compara en este árbol el valor buscado con dos entradas existentes y luego reanuda la búsqueda en una u otra rama. Es este árbol de búsqueda jerárquico se establece que partes del archivo se encuentran en cada sector del disco duro. Así pues, dado que la MFT no es, a diferencia de la FAT, una tabla lineal, durante la búsqueda de un archivo el sistema tampoco debe examinar obligatoriamente toda la estructura. Esto explica el acceso más rápido a archivos de los sistemas NTFS frente a los sistemas de archivos FAT.

Sistemas de archivos UNIX

Los sistemas UNIX utilizan un tipo de sistema de archivos completamente distinto a los tratados hasta ahora. Sólo se puede acceder a estos datos con otros sistemas de archivos Unix o con programas adicionales especiales (NFS−Server, Servidor de sistemas de archivos de red). Los sistemas de archivos Unix no tienen establecida ninguna limitación en cuanto a la longitud de los nombres de archivo, no dividen el disco duro en bloques, como hace FAT, y son muy estables.

La siguiente tabla resume las propiedades de los sistemas de archivos FAT, HPFS y NTFS.

	FAT	**HPFS**	**NTFS**
Nombres de archivo	8+3 caracteres	254 caracteres	256 caracteres
Atributos de archivo	Sin derechos de acceso	Derechos de acceso	Derechos de acceso
Directorios	Sin clasificar	Btree	Btree
Distribución de unidades en varios discos duros	no	no	Sí
Discos espejo	no	Sólo con HPFS 386	Sí
Registro de eventos	no	−	Sí

La tabla siguiente resume con que sistemas de archivos trabajan algunos de los sistemas operativos comentados anteriormente y si estos pueden leer o escribir datos en ellos.

	FAT	**HPFS**	**NTFS**
Windows NT 4.0	Leer y escribir	No compatible	Leer y escribir
Windows NT 3.x	Leer y escribir	Leer y escribir	Leer y escribir
DOS/Windows 3.x	Leer y escribir	−	−
Windows 95	Leer y escribir	Leer con programas	Leer a través de redes adicionales
OS/2	Leer y escribir	Leer y escribir	−
Linux	Leer y escribir	−	−

Métodos para guardar los datos de forma segura

Conjunto de unidades de almacenamiento

Con un conjunto de unidades de almacenamiento se puede reunir espacio disponible en distintos discos físicos (hasta 32), a fin de obtener un único gran volumen con una letra de unidad común. Dicho volumen puede ser dividido en particiones y unidades lógicas, al igual que un disco físico. Los conjuntos de unidades de almacenamiento pueden ampliarse en cualquier momento con más espacio disponible de otros discos duros, sin poner en peligro los datos existentes del conjunto de unidades de almacenamiento. Sin embargo, no es posible reducir el conjunto de unidades sin eliminar los datos que contiene.

Si bien los conjuntos de unidades de almacenamiento permiten un uso eficaz de los discos pequeños o de los espacios disponibles restantes de distintos discos duros, por otro lado, ponen en peligro la seguridad de los datos de todo el sistema. Los defectos de un disco duro físico impiden el acceso a los archivos restantes del conjunto de almacenamiento de datos en cuestión, incluso en otros discos que estén intactos.

RAID

El sistema RAID (Redundant Array of Inexpensive Drives, sistema redundante de discos duros económicos) también reúne, en Windows NT, distintas estrategias para dividir el espacio disponible en diversos discos

duros. De los seis grados de RAID (de 0 a 5), algunos protegen los datos de posibles pérdidas por daños en el equipo, mientras que otros aumentan la velocidad de lectura y escritura. Los procedimientos RAID más conocidos son el RAID 1 y el RAID 5. El RAID 1 duplica los datos en los discos duros idénticos (discos espejo).El RAID 5 forma paridades de conjuntos de bandas, que se distribuyen de forma redundante por todos los discos duros (ver un poco más abajo, en conjunto de bandas). El RAID 5 aumenta el rendimiento en la lectura de datos, pero, en cambio, es más lento que el RAID 1 para escribir. El RAID 5 de Windows NT se controla a través de programa y carga notablemente la memoria principal. Es más efectivo y seguro el RAID 5 del equipo, a través de controladores de discos duros RAID junto con discos intercambiables durante el funcionamiento.

Discos espejo

Con los discos espejo se reproducen los datos de una partición o de una unidad de un disco en un área libre de otro disco duro. Esta área del segundo disco duro deja entonces de estar visible en el administrador de archivos y en la interfaz de comandos, puesto que sólo refleja datos. Los discos espejo son un medio muy eficaz para protegerse contra una posible pérdida de datos debida a un error del disco duro. Sin embargo, de este modo no es posible evitar los defectos de control, los virus y otros problemas, ya que también hacen mella en el conjunto de almacenamiento de datos.

Conjuntos de bandas

En un conjunto de bandas, los datos no se escriben como una totalidad en el disco duro, sino en pequeñas partes denominadas bandas. Los conjuntos de bandas pueden extenderse por distintas áreas de una unidad física (o incluso de distintas**)**.Es posible crear conjuntos de bandas con o sin paridad. Para una banda con paridad es preciso un número impar de partes de espacio disponible (tres o más), mientras que para un conjunto de bandas sin paridad siempre hará falta un número par (dos o más).

Los conjuntos de bandas sin paridad ofrecen ventajas en cuanto a velocidad, porque los datos pueden escribirse al mismo tiempo en distintos discos (quizás utilizando para ello distintos controladores). Si se produce un error en una unidad de almacenamiento de un conjunto de bandas, se pierden todos los datos del conjunto, ya que el resto de bandas, generalmente, no pueden recuperar datos sin la información del defectuoso.

Muy distinto es con bandas con paridad. Aunque con ellas se pierde la ventaja de la velocidad que ofrecen las bandas sin paridad, a partir de la información de paridad se pueden recuperar datos de una banda defectuosa.

El sistema de archivos NTFS

En este apartado analizaremos con más detenimiento el sistema de archivos NTFS, que es el responsable de la organización de los datos en el disco duro en Windows NT.

Windows NT, como sistema operativo de nueva tecnología tenía que incorporar un sistema de archivos de nueva tecnología y despedirse definitivamente del sistema de archivos FAT. Aunque el sistema de archivos FAT, gracias a su ampliación a VFAT, domine los nombres de archivo largos en Windows 95 / DOS 7, apenas cumple los criterios de un sistema de archivos profesional que pueda utilizarse en servidores.

Los sistemas de archivos para sistemas operativos multiusuario y servidor precisan derechos de acceso avanzados para usuarios individuales y para grupos de usuarios.

NTFS permite particiones de disco duro mucho más grandes y archivos como (V)FAT (máximo 4 GB), por lo que está preparado para ser utilizado en servidores. Además, NTFS es compatible con los métodos RAID 1 a 5, que sirven para aumentar la velocidad de acceso y para hacer copias de los datos mediante los discos

duros espejo (ver arriba).

NTFS distingue mayúsculas de minúsculas en los nombres de archivos y directorios y permite caracteres especiales como los acentos. Con ello cumple las directivas del estándar UNICODE.

Las particiones NTFS pueden recuperarse de forma más fácil que las particiones (V)FAT después de un fallo del sistema.

NTFS es menos propenso que (V)FAT a la fragmentación de los discos duros.

NTFS hace patentes sus ventajas en cuanto a velocidad frente a FAT especialmente en cooperación con los controladores SCSI. Gracias al acceso asincrónico a los datos pueden desplazarse procesos de lectura y escritura a las colas de espera, librando así al procesador de una carga. Durante la edición de un proceso pueden aceptarse y editarse entonces otros procesos. Especialmente en servidores Windows NT, que tienen que afrontar numerosos procesos de lectura y escritura debido a los accesos simultáneos de los usuarios, es donde NTFS experimenta un aumento de velocidad más evidente en controladores SCSI de 32 bits.

Hasta la versión 3.51, Windows NT era compatible con el sistema de archivos HPFS. Este sistema de archivos desarrollado originalmente por Microsoft se sigue suministrando actualmente con OS/2. HPFS es tan seguro como NTFS y en su ampliación para WARP Server muestra las mismas propiedades en cuanto a compatibilidad con RAID y derechos de acceso. Lamentablemente, desde la versión 4.0 Windows NT sólo puede leer particiones HPFS y convertirlas en otras particiones, pero no puede crear particiones HPFS propias o escribir en ellas.

Organización de los datos en NTFS

NTFS, a diferencia de otros sistemas de archivos, no utiliza bloques fijos para los archivos de parámetros o de inicio. Únicamente un bloque de parámetros BIOS establecido y definido por el hardware debe incorporarse en un lugar fijo del disco duro. Los archivos de inicio y el resto de archivos para la organización del sistema pueden estar en cualquier lugar del disco duro. De esta forma los datos y sobretodo la capacidad de inicio de un disco duro, están mejor protegidos ante errores de hardware del disco duro y de sus efectos. Físicamente, NTFS divide el disco duro en clústers. El tamaño de los clústers puede indicarlo uno mismo al dar formato al disco duro o bien puede configurarlo automáticamente NTFS a partir del tamaño de disco disponible.

El papel central de la organización de archivos NTFS es el de la tabla principal de archivos (MTF). Esta tabla contiene para cada archivo un registro (registro MFT) que a su vez contiene los atributos de archivo y los datos sobre qué partes del archivo se pueden encontrar en qué clústers del disco duro. Existe una copia de seguridad de la MFT, que puede utilizarse para reconstruir los datos en caso de error en el disco duro. La MFT y su copia de seguridad pueden colocarse en un lugar cualquiera del disco duro, es decir, pueden estar separadas por áreas de datos de cualquier tamaño y por los sectores de parámetros del disco duro. La MFT es un archivo NTFS completamente normal y el sistema de archivos lo administra como si se tratara de cualquier otro archivo.

Cada registro MFT tiene exactamente un tamaño de 2 KB y contiene los datos siguientes:

Un encabezado con datos internos del sistema de archivos, en el que se guarda, por ejemplo, cuantos otros archivos o directorios remiten al archivo o directorio actual.

Información sobre atributos del archivo y sobre su nombre.

Las referencias a los sectores en los que se encuentran las distintas partes de un archivo.

Atributos de seguridad avanzados del sistema de archivos NTFS.

Los atributos y el encabezado del registro MFT ocupan unos 560 bytes, de modo que para las referencias a los sectores en los que se encuentra el archivo quedan unos 1,44 KB disponibles. Para no regalar espacio, los archivos pequeños (de menos de 1,44 KB) se guardan en la propia MFT, por lo que las referencias son sustituidas por los datos auténticos.

En cambio, para archivos muy grandes o fragmentados no son suficientes los 1,44 KB para poder guardar todas las referencias al archivo. En tal caso se crean para el archivo otros registros MFT que guardan las referencias adicionales. Estos registros ya no contienen entonces información sobre los atributos de archivo. Es el registro MFT original se encuentran ahora, en lugar de las referencias a los clústers del archivo o del directorio, las referencias a los otros registros MFT. En este caso las referencias se denominan atributos externos.

En NTFS los directorios son tratados como archivos, igual que en la mayoría de sistemas de archivos, sólo que contienen otro atributo. El contenido de un directorio se guarda en el registro MFT como un índice compuesto por el nombre de los archivos y subdirectorios y un número único de archivos o directorios. Si este índice tiene menos de 1,44 KB, se encuentra directamente en el registro MFT. Los archivos de índices mayores son guardados como si fueran archivos y directorios grandes, de modo que en el registro MFT original sólo hay referencias a otros registros MFT, que son los que contienen realmente los datos.

De esta manera, para cada directorio se guardan en forma de árbol los archivos y subdirectorios que contiene. Esto es lo que se denomina árbol binario. Estas referencias directas a los archivos de un directorio desde el propio directorio permiten un acceso a los datos mucho más rápido. En una FAT, para buscar un archivo primero debe examinarse completamente toda la tabla (sin ordenar). En cambio, en un árbol binario (ordenado) se accede al archivo deseado directamente desde el directorio.

Como evitar nombres de archivo 8+3

Si utiliza programas DOS o WIN 16 en Windows NT no puede servirse de los nombres de archivo largos de NTFS. Dado que de forma predeterminada para cada archivo se guarda el nombre DOS 8+3, estos programas utilizan ese nombre. Cuando guarde un archivo con un nombre de archivo largo con este programa DOS, por desgracia se perderá el nombre largo e incluso algunos atributos de archivo NTFS.

Esto puede evitarse prohibiendo totalmente guardar archivos en formato 8+3 en Windows NT. Para ello debe definir con el valor 1 la entrada *NtfsDisable8dot3NameCreation* de la base de datos de registro de Windows NT. Encontrará esta entrada en la base de datos de registro dentro del árbol

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

Administración de unidades de almacenamiento en Windows NT

La administración de discos duros es especialmente interesante para servidores. Los servidores disponen de varios discos duros, generalmente mucho más grandes que los ordenadores de escritorio. Los datos de esos discos duros no sólo deben ponerse a disposición de los clientes, sino que también deben de estar guardados en los discos duros de forma segura.

Tamaño de los discos duros: el tamaño de los discos duros no es asunto del sistema operativo instalado. Sin el controlador Enhanced IDE o LBA BIOS pueden surgir problemas con los discos IDE, ya que sólo son iniciables las particiones por debajo de 540 MB. En los discos SCSI no hay este tipo de problemas.

Seguridad: de la seguridad de los datos de un disco duro se encarga, esencialmente, junto con la calidad del

disco duro en sí, el sistema de archivos. La seguridad de los datos comprende, además de lo mencionado, un buen plan de seguridad y una copia de seguridad.

Velocidad de acceso: es necesario procurar una velocidad de acceso suficiente, a fin de que el trabajo con unidades de red no ponga a prueba la paciencia del usuario. La velocidad de acceso no sólo es cuestión del disco en sí y del controlador de disco duro, sino también del sistema de archivos y particiones.

Windows NT ofrece un programa adicional propio para la administración de discos duros, el *Administrador de discos.*

EL administrador de discos

El administrador de disco es la herramienta gráfica que emplea NT para la gestión de discos duros, con dicha herramienta podemos:

Gestionar particiones de disco y unidades lógicas.

Dar formato a volúmenes y asignarles nombres.

Leer la información del estado de los discos.

Leer la información del estado de los volúmenes, la etiqueta y la letra del volumen, el sistema de archivos y su tamaño.

Crear y modificar las asignaciones de letras.

Ampliar un volumen o un conjunto de volúmenes.

Crear y eliminar conjuntos de volúmenes.

Crear o eliminar conjuntos de bandas con o sin paridad.

Regenerar un miembro no encontrado de un conjunto de bandas.

Establecer o romper conjuntos de espejos.

Antes de comenzar un par de advertencias: el administrador de discos no permite trabajar sobre la partición de sistema (normalmente C:), ya que contiene los archivos necesarios para que NT se ejecute, el resto de las particiones son totalmente moldeables pero tendrá que tener cuidado con lo que hace en aquellas que contengan datos, ya que podría perderlos.

En este gráfico puede ver al administrador de discos trabajando sobre un sistema con tres discos físicos (0,1 y 2) y un lector de CD−ROM, aquí puede apreciar:

Una partición primaria y activa de 515 MB que contiene la unidad lógica C: en el disco duro 0.

Un conjunto de espejos para integridad de datos (unidad D:) en el disco duro 1.

Una unidad lógica repartida en dos particiones de dos discos distintos, el 0 y el 1,(conjunto de volúmenes J:). Fijarse en que aun está sin formatear.

Un disco duro con cinco particiones: tres de unidades lógicas E: , F: , G: y un espejo de la unidad D: del

disco 1.

Espacio disponible sin particionar en el disco 2.

Con esta configuración hemos conseguido:

Realizar un espejo (o sea una copia exacta) de un volumen (D:)que contiene los datos más importantes almacenados en este servidor, si mañana me falla uno de los discos duros puedo romper el espejo en el que ha quedado funcionando y seguir trabajando como si nada, incluso podré hacer un nuevo espejo con un tercer disco duro que siga en funcionamiento.

Hemos aprovechado el espacio sobrante en dos discos duros para crear un solo volumen (J:) de mayor capacidad.

También existe una zona sin asignar de 47 MB que podemos utilizar con total libertad para ampliar cualquiera de los volúmenes que se nos quede pequeño.

Y todo esto se ha realizado usando solamente el administrador de discos y una cierta planificación a la hora de adquirir los discos duros para el equipo (mejor dos o tres más pequeños que uno sólo más grande). También es muy importante saber como particionar correctamente un disco duro antes o durante la instalación de NT.

El entorno de trabajo

Para empezar dele un vistazo a estas dos imágenes. Nos dicen casi lo mismo pero en distinto formato, son los dos tipos de vista que puede utilizar:

El modo de vista "Volúmenes" resalta más las unidades lógicas y es más completa en cuanto a datos numéricos como la capacidad, el espacio disponible y el porcentaje de espacio disponible en relación a la capacidad total, datos muy interesantes para ver que volúmenes se están quedando pequeños y como tiene repartido el espacio de almacenamiento.

La vista "Configuración de disco" muestra como están organizadas las particiones y volúmenes dentro de los discos físicos, es la más adecuada para el trabajo fuerte con el administrador de discos, o sea, extender volúmenes, crear o eliminar particiones, establecer espejos, etc. Es la que usaremos a lo largo de estas páginas.

En esta última imagen puede ver de una manera muy intuitiva como está repartido el espacio en el disco duro. Cada cuadradito representa un volumen, los códigos de colores indican como está configurado cada volumen, también aparecen aquí la etiqueta, el tipo de formato y el espacio total. El significado de cada color viene dado por la leyenda de la penúltima barra que puede configurar desde el menú Opciones.

Si pulsa con el ratón sobre alguno de los cuadritos que representan los volúmenes lo habrá seleccionado para poder trabajar con él, deje pulsada la tecla de mayúsculas y pulse en nuevos cuadritos si quiere seleccionar varios a la vez, del mismo modo puede seleccionar las zonas rayadas que representan el espacio disponible no asignado a ningún volumen.

Truco: pulsando el botón secundario del ratón sobre cualquier cuadrito accedes a un pequeño menú con las tareas que pueden realizarse sobre dicho volumen.

Las acciones que vaya realizando no serán efectivas hasta que registre los cambios que ha hecho, esto, que a veces despista o resulta tedioso, es una buena medida de seguridad frente a la pérdida de datos. Para realizar determinadas acciones (por ejemplo formatear un volumen después de crearlo) tendrá que ir confirmando los

cambios sobre la marcha usando el comando Partición/Registrar cambios ahora. Si sale del programa sin haber registrado los cambios un diálogo le dará la posibilidad de hacerlo o de salir sin registrar nada.

Guardar datos

En los apartados anteriores he presentado distintas posibilidades de proteger los datos de forma activa. En este caso, hablamos de protección activa porque estas medidas evitan las perdidas de datos. Ahora trataremos las medidas de seguridad pasivas con las cuales se reducen al mínimo las consecuencias de una pérdida de datos. Una de las medidas de seguridad pasivas consiste en guardar periódicamente los datos en otros soportes de datos.

Aquí haré referencia a verdaderas unidades de copia de seguridad.

Elegir el medio

Una de las primeras cuestiones a considerar para guardar datos es la elección del medio de almacenamiento correcto. Se dispone de los medios siguientes, entre otros, con distintas capacidades de almacenamiento:

Cintas de copia de seguridad de hasta 500 MB.

Cintas DAT (DDS1, DDS2) de hasta 2 o 4 GB, comprimidas hasta 4 u 8 GB (en función del medio: cinta DAT de 90 o 120 metros).

Cintas DLT de hasta 20 o 40 GB.

Unidades magnetoópticas hasta 900 MB.

CD−ROM con hasta 600 MB.

Discos intercambiables mínimo 1 GB.

El tamaño de los datos reduce la selección de las posibles unidades de almacenamiento. En cualquier caso, también se deben tener en cuenta la durabilidad y el manejo de los medios. Los CD−ROM grabados por uno mismo duran mucho menos que los editados por los fabricantes. La capa del cd en la que se escribe es muy delicada y puede que dar inutilizable con sólo algunos rasguños. Además actualmente algunos críticos de estos medios predicen unos pocos años de durabilidad incluso tratándolos con cuidado ya que los cd de plástico se descomponen.

Los CD−ROM gozan de la decisiva ventaja de que sólo con introducirlos en una unidad de CD−ROM se puede trabajar con los datos. Por lo tanto, se puede prescindir de la reproducción de los datos tal y como sucede son una unidad de cinta.

Las unidades MLO son muy seguras, puesto que los datos se escribes en el medio bajo un determinado aumento de temperatura. En cuanto el medio se enfría, no puede dañarse, por ejemplo, con un imán.

Las cintas son un medio de almacenamiento de gran durabilidad. Para almacenar datos en una cinta, lo que se denomina copia de seguridad se debe escribir en ella con un programa especial y para leer los datos se debe utilizar el mismo programa.

Precisamente sobre esta cuestión, las empresas no deben elegir cualquier programa ni cualquier unidad para realizar copias de seguridad sino utilizar estándares que sean soportadas durante las dos décadas siguientes. Si opta por una unidad SCSI−DAT utilizando el programa para copias de seguridad de Windows NT, hasta

cierto punto puede estar seguro de que estas copias podrán leerse con versiones posteriores de NT. Lo mismo se puede aplicar para proveedores conocidos, que vendan programas de este tipo desde hace años.

Copias de seguridad de Windows NT

Windows NT contiene, en su versión estándar, un sencillo programa de copias de seguridad de la casa Seagate, el fabricante de Arcada Backup para NT. Con el mismo se pueden guardar datos en unidades de cinta compatibles con Windows NT y previamente instaladas en Windows NT.

Información

El programa de copias de seguridad de Windows NT no soporta el almacenamiento en disquetes.

En Windows NT también se pueden iniciar copias de seguridad con el comando backup de la interfaz de comandos. De esta forma, es posible iniciar copias de seguridad fácilmente, a través de conexiones remotas con el ordenador Windows NT.

Almacenamiento de datos con el programa de copias de seguridad de NT

Inicie el programa *Copia de seguridad* en el menú *Herramientas administrativas*. Durante el inicio el programa intenta rápidamente detectare y mostrar las unidades de cinta instalada.

En la ventana *Unidades* obtendrá una relación de las carpetas y archivos del ordenador y de las unidades de red vinculadas.

Pulsando dos veces el icono de la unidad se muestran las carpetas de la misma en una nueva ventana. En ella puede seleccionar los directorios que quiera copiar. Si ya ha seleccionado previamente la unidad, estarán seleccionados todos los directorios. Para anular esta selección deberá pulsar la casilla que se encuentra en la esquina superior izquierda.

Luego, pulse el botón *Copia de seguridad* he indique el nombre y otros particulares para la copia de seguridad.

Programas para copias de seguridad

A título de ejemplo de un buen programa para copias de seguridad, describiré aquí el ARCserve y Arcada Backup Exec para Windows NT. Con ARCserve de la casa Cheyenne se pueden administrar varios servidores de forma centralizada. A través de acceso remoto (RAS) es posible modificar la configuración de ARCserve he iniciar tareas de copias de seguridad. De este modo, ARCserve funciona como servicio del sistema y, por lo tanto, no precisa ningún usuario conectado. Gracias a la división del proceso de tareas, proceso de cinta y proceso de base de datos, se garantiza una alta estabilidad y velocidad. Para incrementar la velocidad de la copia se puede acceder, de forma paralela a distintos dispositivos de copia de seguridad. Un detector de virus hace posible la integridad de los datos antes de la copia. Además, se puede consultar información sobre destinatarios de llamadas, correo electrónico, colas de impresión, SNMP o mensajes de red.

Arcada Backup Exec es un producto de la firma Seagate. En Arcada Backup se instalan y planifican las tareas a través del programa Backup Exec. A través de RAS puede iniciar de modo remoto trabajos de copia de seguridad con Backup Exec View y comprobar si las copias se han realizado correctamente.

Arcada Backup se luce por su integración en Windows NT. Por ejemplo: todos los eventos importantes del sistema se escriben directamente en el registro de aplicaciones de NT.

Discos duros fragmentados

Los discos duros guardan los datos en sectores, de forma consecutiva. El disco duro se va llenando con datos de este modo. La información sobre que partes de un archivo se encuentran en que sectores esta guardada en la tabla de asignación de archivos. En el sistema de archivos NTFS este archivo se denomina Master File Table (MFT).

Cuando se eliminan archivos se comparten las áreas correspondientes, aunque estas no pueden ser sobrescritas realmente hasta que se agota el espacio al final del disco duro. En este preciso momento surge el problema de la fragmentación de archivos. Si las áreas disponibles son más pequeñas que el archivo a guardar, es preciso dividir el archivo en varias áreas, es decir, subdividirlo en fragmentos. Cuanto mayor es la frecuencia con que se eliminan, reducen y amplían archivos, más fragmentos se van formando en el disco duro.

Además de la fragmentación de archivos, puede producirse una fragmentación del soporte de datos. Si el disco duro ya ha llegado una vez a su límite de capacidad, sólo es posible compartir espacio eliminando o reduciendo archivos. Pero, como es natural, lo que se hace es dividirlo en pequeños fragmentos.

En NTFS, la fragmentación de archivos no juega un papel tan importante como en el sistema de archivos (V)FAT. Debido a una organización de los datos algo diferente, los discos duros NTFS no se fragmentan tan rápidamente como los que tienen el sistema (V)FAT. Sin embargo, en servidores cuyos datos se escriben y se modifican con frecuencia, pueden producirse fragmentaciones que retardan notablemente el acceso a los datos.

Programas defragmentadores

Para volver a organizar el disco duro dividido en fragmentos y escribir los archivos seguidos en lo posible es necesario un programa defragmentador. Este tipo de programas pueden trabajar fuera de línea y en línea. Las defragmentaciones fuera de línea no permiten ningún acceso a los archivos durante la reorganización del disco duro. Así, por ejemplo, en una estación de trabajo pueden ejecutarse durante un funcionamiento en vacío o al apagar o encender el ordenador.

Para un servidor, estos programas defragmentadores fuera de línea no son tan adecuados. Todo administrador de sistema causará la irritación de sus compañeros si tiene que parar el sistema con mucha frecuencia, y trabajar por la noche o en domingo tampoco es un medio adecuado.

En estos casos, es preciso recurrir a los defragmentadores en línea, que permiten acceder a los datos mientras se están escribiendo y, a pesar de ello, trabajan de forma fiable. Es fácil imaginarse que un programa de este tipo no es fácil de crear y que con un programa que funciona de forma imperfecta es uy fácil dañar todos los datos de un disco duro.

Microsoft no ofrece un programa defragmentador para NTFS, como ocurre con el sistema de archivos (V)FAT. En este caso hay que recurrir a la ayuda de otros fabricantes. Ya existen defragmentadores sencillos como el shareware o freeware. Para uso empresarial es mejor recurrir a las versiones comerciales ampliadas de estos programas, puesto que la mayoría de ellas permiten la terminación de la defragmentación y también son adecuadas para la administración remota.

Como ejemplo de estos programas citamos Diskeeper de Executive Software.

Sistema de archivos distribuido

Con el Sistema de archivos distribuido (DFS), es posible administrar y utilizar recursos en redes grandes de modo más fácil y claro. Con DFS pueden activarse los recursos compartidos de muchos ordenadores distintos

en una red a través de una estructura unitaria. Con DFS ya no es preciso pelearse con largos árboles con dominios, ordenadores y recursos compartidos, sino que se utiliza una jerarquía unitaria para acceder a dichos recursos.

Así trabaja DFS

Hasta ahora se utilizaba en Windows NT, al igual que en otros sistemas operativos Windows, el Universal Convenrion System (UNC) a fin de nombrar los servidores y los recursos. En general, la dirección de un archivo en la red tiene entonces este aspecto:

En general...

\\Servidor\Recurso\Ruta *de acceso al directorio\Nombre de archivo*

o con un ejemplo...

\\SERVIDOR *NT 1\USUARIO\LUIS\PRIVADO\LIBRO.XLS*

Se puede asignar a los recursos una determinada letra de unidad en el cliente de la red. Windows lo denomina entonces *Vincular una unidad de red.* El aspecto es el siguiente:

En general...

X:\Ruta de acceso al directorio\Nombre de archivo

o en nuestro ejemplo

X:\LUIS\PRIVADO\LIBRO.XLS

Algunos programas no pueden trabajar con un sistema puramente UNC, por lo que es necesario vincular siempre una unidad con un determinado recurso.

En redes grandes con numerosos servidores y estaciones de trabajo que dan a compartir muchos recursos distintos, el sistema UNC resulta poco claro. Para encontrar un determinado recurso es preciso

conocer el servidor que lo contiene

descubrir en él el recurso y

localizar el archivo correcto dentro del árbol de directorios de ese recurso.

Para vincular todos los recursos necesarios con una unidad no hay suficiente con las letras del abecedario. Además, estas unidades de red vinculadas de forma fija consumen unos valiosos recursos del sistema, por lo menos en Windows 3.11 y Windows 95.

DFS presenta los distintos recursos de los servidores de una red con una estructura jerárquica unitaria. En ella es posible clasificar los archivos y directorios por contenido y no es preciso tener en cuenta el espacio físico.

DFS se comporta un poco como el sistema de archivos de un soporte de datos. No es preciso que uno mismo compruebe los distintos bloques en los que se guarda un archivo −tal vez fragmentado −, sino que únicamente se selecciona el archivo. El sistema de archivos busca entonces los datos en sí en los bloques del soporte de datos.

Con DFS, el usuario tampoco tiene que buscar mucho rato un archivo determinado si el mismo se ha trasladado a otro directorio o a otro servidor por razones de organización. Dado que la entrada del DFS para ese archivo sigue siendo la misma, se sigue presentando con la misa dirección para los usuarios (independientemente del ordenador y el directorio en los que se encuentre realmente).

Como es natural, DFS no sólo ofrece ventajas para los usuarios. Los administradores del sistema también se aprovechan del hecho de que DFS amplía las configuraciones de seguridad del servidor Windows NT a todos los recursos compartidos. Por lo tanto, ya no es preciso pensar en unidades FAT compartidas sin protección. En entornos heterogéneos, DFS permite observar de forma unitaria las unidades y los directorios de los ordenadores compatibles (FAT, HPFS, NTFS) y estaciones de trabajo Unix (NFS y otros sistemas de archivos Unix). Así pues, los usuarios ya no necesitan clientes NFS adicionales ni tendrán que administrarlos.

Finalmente, DFS puede acelerar notablemente el acceso a los recursos mediante el almacenamiento temporal de los recursos de red activados una vez.

6 WINDOWS NT EN LA RED

Las empresas trabajan con sistemas operativos de red muy diversos.

Windows NT trabaja en redes:

como servidor de una red puramente Windows NT

como cliente eficaz de redes Windows NT, Netware, Banyan Vines o heterogéneas

como servidor de aplicaciones (por ejemplo, para bases de datos)

como Gateway (por ejemplo, para la integración en host IBM) y

como intermediario entre distintos sistemas operativos de red.

En este capítulo se describe la filosofía de red de Microsoft para Windows NT y los fundamentos de las redes con Windows NT.

La administración de redes Windows NT y el trabajo es redes heterogéneas se tratarán en capítulos posteriores.

6.1 Filosofías de red

Windows NT Server es un sistema operativo de red. Es por ello que en este capítulo se explican, en primer lugar, los conceptos esenciales de redes y se muestran cuáles son los que utiliza Windows NT. También se aclara la diferencia entre redes punto a punto y redes de servidor con Windows NT Server.

La idea de las redes

Las redes pueden cumplir distintas tareas. Si bien anteriormente las redes ofrecían varios recursos informáticos de elevado coste (discos, impresoras, módems, trazadores gráficos), actualmente se encargan de otras muchas tareas.

Las redes permiten en la actualidad:

poder trabajar hasta cierto punto con independencia del equipo informático y de la ubicación del propio lugar de trabajo

acceder en cualquier momento a recursos (discos duros, memoria RAM, impresoras,...) seleccionados en una red e

iniciar, en otros ordenadores, aplicaciones que no están instaladas en el propio ordenador.

Además, las redes ofrecen:

comunicación e información a nivel mundial

interfaces y

edición común de tareas dentro de la red.

Las redes se utilizan actualmente de forma muy intensiva, tanto dentro de las empresas como fuera de sus límites. Cuando se trabaja con datos delicados en la red de una empresa, que también es accesible desde fuera mediante una conexión con Internet, se requieren unas medidas de seguridad particularmente escrupulosas. Aquí mostraré las características de seguridad de Windows NT como servidor en una red.

Construir redes

Si se instala una red de forma totalmente objetiva, su aspecto puede ser muy simple: los usuarios de la red pueden utilizar los recursos de la misma. Para ello basta con que el usuario comunique sus deseos a otros ordenadores y espere a que esos recursos estén disponibles. El ordenador COMPI−A dispone de un disco duro muy grande y, por lo tanto, puede ofrecer espacio al resto de ordenadores de la red. Para hacer uso de ese espacio, el usuario del ordenador COMPI−C da la instrucción: utiliza el disco duro con la denominación HD_01 del ordenador COMPI−A.

En este caso, COMPI−C parte del hecho de que puede utilizar cualquier recurso del otro ordenador y de que conoce el nombre del resto de ordenadores y de sus recursos.

En grandes redes de empresas, raras veces se pueden encontrar ordenadores conectados punto a punto con iguales derechos.

El concepto opuesto de red es el que empleaban los ordenadores Mainframe con equipos informáticos enormes y usuarios con terminales tontos, que utilizaban la memoria y la capacidad de cálculo del ordenador central y, por ellos mismos, no podían procesar ni guardar datos de forma local.

Actualmente, las redes, salvo pocas excepciones, trabajan según el principio cliente−servidor. Determinados ordenadores ofrecen los recursos y controlan la utilización de los mismos, mientras que unos terminales inteligentes (los clientes) recurren a los recursos del servidor, pero también pueden trabajar de forma autónoma. Las redes cliente−servidor pueden estar organizadas centralmente de distintas formas.

Estructuras cliente−servidor

En redes basadas en el principio cliente−servidor, los servidores ponen a disposición de sus clientes recursos, servicios y aplicaciones. Dependiendo de que recursos ofrecen los servidores y qué recursos conservan en los clientes, se pueden distinguir distintas estructuras cliente−servidor en función del lugar:

donde se encuentre los datos

donde se encuentren los programas de aplicación y

donde se presenten los datos.

A continuación se presenta una introducción a estos conceptos

Sistema central basado en el host

Los datos, programas de aplicación y la presentación se encuentran en el servidor. La imagen final se envía a terminales simples para el usuario. Los terminales vuelven a enviar las cadenas de caracteres de las entradas de usuario al host. Los sistemas Mainframe están basados en este concepto.

Downsized − PC−Cliente/Servidor (host)

Los datos y aplicaciones se guardan de forma central en el servidor, Los datos se consultan a través de las aplicaciones que guarda el propio servidor. Las estaciones de trabajo son simplemente equipos basados en Windows.

Rightsized − estación de trabajo−Cliente/sevidor de base de datos

En el servidor se encuentran los datos (generalmente en una base de datos). Con un cliente de la base de datos se accede a esos datos desde el ordenador de cualquier lugar de trabajo. En el cliente se procesan los datos utilizando para ello la inteligencia del cliente. Cada estación de trabajo contiene, de forma local, aplicaciones con las que luego se pueden procesar los datos.

Smartsized PC Cliente/Servidor de aplicaciones

En este tipo de red, como mínimo, se dispone de dos servidores distintos. Un servidor actúa como mero servidor de base de datos, y el resto como servidores de aplicaciones. En esta red, los servidores de aplicaciones también son responsables del acceso a la base de datos. En cada estación de trabajo se ejecutan las aplicaciones clientes correspondientes.

Sistema Cliente/Servidor descentralizado cooperativo

A diferencia de la reds Smartsized, la base de datos está distribuida en distintos servidores o incluso clientes. Las aplicaciones funcionan igualmente en varios servidores o, en parte, en clientes.

En las redes Windows NT no se aconseja probar la primera variante (sistema central), muy rígida; esta se deja para los ordenadores Mainframe. Todos los grados de descentralización restantes se pueden encontrar en redes puramente NT o incluso en entornos heterogéneos.

6.2 Conceptos de red de Microsoft

Microsoft empezó a tratar el tema de redes casi de cero. Las primeras ampliaciones de red para MS−DOS, realmente no ofrecían mucho más que lo que se ha descrito al principio con el concepto más simple. Sin embargo, pronto se encontró muy limitado. Cuando había muchos ordenadores se perdía la visión de conjunto y no se podía saber quién estaba utilizando cada recurso. Además, era necesario apuntarse todos los nombres y direcciones posibles para registrarse individualmente para cada recurso.

Este camino condujo a las redes, aún hoy utilizadas, Windows para trabajo en grupo, las redes punto a punto. En ellas, existen unos subgrupos de ordenadores conectados que forman grupos de trabajo. Los ordenadores de un grupo de trabajo pueden utilizar recursos mutuamente. Cada usuario puede decidir, por sí mismo, qué

recursos de su ordenador quiere ofrecer a los miembros del grupo de trabajo y qué recursos no. La utilización de archivos y directorios esta graduada mediante simples derechos de acceso. Sólo es posible pasar a otros grupos de trabajo de la misma red registrándose en la red en cuestión. Un grupo de trabajo no puede evitar que un miembro de otro grupo se registre y utilice los recursos compartidos. En las redes punto a punto de Microsoft, no existe ninguna instancia central para el control de los derechos de acceso y las utilizaciones en la red. Únicamente la Personal NetWare de Novell separa rigurosamente entre sí los grupos de trabajo, incluso en redes punto a punto.

Estas limitaciones muestran posibles ámbitos de aplicación del concepto punto a punto: en redes totalmente cerradas formadas por pocos ordenadores sin datos de transcendencia comercial, las redes punto a punto, como por ejemplo Windows para trabajo en grupo, prestan perfectamente su servicio. No obstante, la falta de concepto de seguridad y las limitaciones de acceso convierten su utilización en el ámbito empresarial en un riesgo de seguridad inexcusable. Las leyes de protección de datos tampoco se pueden tener en consideración en la extensión que requiere la legislación.

La respuesta a ello son las redes cliente−servidor, en las cuales como mínimo un ordenador asume el papel de vigilante y coordinador. Mientras un grupo de trabajo no es nada más que el nombre de un grupo de ordenadores que comparten ciertos recursos, detrás de un dominio hay un grupo de ordenadores que poseen un concepto de seguridad común. Este es administrado por un servidor del dominio, el controlador principal de domino. Por lo tanto, hay dos novedades esenciales:

Existe un servidor. Esto significa que no todos los ordenadores tiene los mismos derechos.

Cualquier ordenador físicamente conectado no puede utilizar los recursos del grupo de trabajo si no dispone de una autorización de acceso al dominio.

Microsoft ha aplicado este concepto de red en la red Windows NT. La posición central la toma aquí el controlador principal de dominio, un servidor NT. Puede estar representado por un servidor sustituto, el controlador de dominio de reserva o controlador de dominio de seguridad. Estos servidores responden al concepto de seguridad y administran los recursos disponibles de forma centralizada. Además, las redes NT también pueden contener otros servidores como simples servidores de archivos o de aplicaciones. Éstos también se incluyen en el concepto de seguridad de Windows NT a través de los controladores de dominio.

En las redes Windows NT pueden utilizarse los siguientes sistemas operativos o conexiones de red para clientes u otros servidores:

MS−DOS con expansión de red

Windows para trabajo en grupo

Windows 95

Windows NT

OS/2 incluyendo LAN−Manager

Novell NetWare y

Mac System 7.x (sólo cliente).

6.3 Protocolos de red

En las redes intercambian datos ordenadores con sistemas operativos muy distintos. En el sentido físico, esto tiene lugar a través de tarjetas adaptadoras en los ordenadores, las denominadas tarjetas de red, y una conexión entre las tarjetas de red (generalmente un cable, pero también puede tratarse de conexiones por radio o láser). Cada capa es controlada por distintos programas, denominados protocolos. Algunos de ellos sirven únicamente para transportar datos, mientras que otros se ocupan de la comunicación entre los ordenadores y otros de la conversión de los datos cuando ambos ordenadores utilicen distintos juegos de caracteres, por ejemplo.

Como cualquier componente periférico, las tarjetas de red también necesitan programas controladores para comunicarse con Windows NT. Los controladores de red ocupan una de las capas de protocolo inferiores. Este tipo de controladores contienen, entre otras cosas, información acerca de qué interrupción y qué dirección de memoria utiliza una tarjeta.

Información

Las tarjetas de red PCI modernas asignan estos valores automáticamente, las direcciones de memoria, en parte, no se utilizan más. Esto no sólo facilita la instalación, sino que también evita conflictos con otros componentes.

Hasta ahora he descrito las condiciones físicas para que los ordenadores estén conectados entre sí y puedan enviarse y recibir datos a través de los controladores. En este punto falta asegurar que los ordenadores conectados hablen el mismo idioma, y, por lo tanto, realmente puedan intercambiarse datos entre sí. De este trabajo se encargan los protocolos de red.

Los protocolos de red comunican a un ordenador cómo y con qué avisos previos debe enviar sus datos. Al destinatario le comunican sobre qué información debe reaccionar y cómo debe hacerlo. Como no podía ser de otro modo, no todas las redes utilizan el mismo protocolo, sino que existe un gran número de protocolos de red distintos (condicionados por la historia, los fabricantes utilizan determinados protocolos; Novell: IPX/SPX, Microsoft: NetBIOS/NetBEUI así como MS−TCP/IP, UNIX, Internet: TCP/IP).

Afortunadamente, es posible instalar protocolos para una tarjeta de red y utilizarlos de forma paralela. Windows NT soporta los protocolos de red relacionados en la siguiente tabla.

Protocolo	**Descripción**
NetBIOS/ NetBEUI	NetBIOS (Network Basic Input Output System) es el protocolo más simple. Fue desarrollado en los tiempos de las redes MS−DOS por Microsoft y consta de menos de 20 comandos sencillos que se ocupan del intercambio de datos. Pronto fue perfeccionado y ampliado adoptando un nuevo nombre, NetBEUI (NetBIOS Extended User Interface). Sigue utilizando el juego de comandos NetBIOS.
Nwlink	A partir de Windows NT 3.5x se introdujo adicionalmente al protocolo NetBEUI el protocolo Nwlink, que es compatible con Netware. Este protocolo compatible con SPX/IPX puede encargarse del transporte de los datos en una red, igual que NetBEUI o TCP/IP. Con el protocolo Nwlink es posible darse de alta con un ordenador Windows NT directamente como cliente en una red Novell. Sin embargo, los recursos de esta red (archivos, periféricos) sólo se pueden utilizar cuando se ha instalado el servicio Gateway de Netware.
TCP/IP	TCP/IP es la abreviatura de Tranmission Communication Protocol Internet Protocol y ya indica claramente de dónde procede este protocolo. El protocolo TCP/IP sirve para construir intranets y conexiones con Internet

	en LANs. TCP/IP es un protocolo orientado por paquetes muy eficaz, que fue desarrollado en los años setenta por el Pentágono para construir redes a prueba de fallos. Actualmente, este protocolo se ha desarrollado a nivel mundial en Internet. TCP/IP es una extraordinaria plataforma para protocolos de las aplicaciones y servicios más variados que se pueden conseguir a través de la red. TCP/IP desplaza cada vez más al resto de protocolos.
DLC	El protocolo DLC (Data Link Control) se apoya en un estándar industrial (IEEE 802.2) y sirve para la comunicación entre Windows NT y ordenadores Mainframe o componentes de red especiales como tarjetas JetDirect de HP o tarjetas Markision de Lexmark.
IPX/SPX	IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange) es el protocolo de las redes Netware, ampliamente extendido en LANs. Las versiones anteriores de Windows NT no soportaban este protocolo. El mismo no formó parte de los servicios de compatibilidad con Netware hasta la versión 3.5 de Windows NT.

Por lo tanto, Windows NT soporta muchos protocolos de red distintos. De esta forma, cumple un requisito esencial para su utilización en redes heterogéneas. Los servicios y Gateways adicionales de Microsoft (Netware−Gateway−Service, SNA) se ocupan de que se puedan utilizar todos los recursos de otros conceptos de red.

6.4 Conceptos de seguridad que sobrepasan los dominios

Como cliente de un dominio Windows NT tal vez quiera utilizar al mismo tiempo los recursos de distintos dominios con los que exista una conexión física. Sin ninguna configuración adicional, una red Windows NT no lo permite, ya que sólo se puede estar registrado en un dominio a la vez. Esto se aclara con el ejemplo siguiente.

Consideramos una red sencilla con dos dominios, *Compras* y *Ventas.* Estas dos subredes están conectadas físicamente entre sí. Sin ninguna otra configuración, los usuarios no pueden utilizar ningún recurso del otro dominio ni registrarse desde uno de sus ordenadores en el otro dominio.

No obstante, al señor X, de compras, le gustaría acceder a las ventas del último mes para planificar mejor las compras. Naturalmente, siempre podría pedir que Ventas le enviara esa lista por correo interno. Pero es complicado, tarda demasiado y la lista no contiene las modificaciones actuales. Para un acceso en línea, el señor X tendría que acceder directamente a la base de datos de ventas.

Para ello, el dominio *Ventas* debe construir una posición de confianza con el dominio *Compras*. Esto permitirá a los miembros del dominio *Compras* acceder a determinados recursos compartidos para ellos del dominio *Ventas.*

A fin de que los usuarios del dominio *Compras* puedan iniciar la sesión en el dominio *Ventas,* deben disponer de una autorización de acceso en el mismo. Con la misma, el señor X podrá acceder a los recursos del dominio *Ventas*. Sin embargo, hasta ahora ha tenido que darse de alta y de baja continuamente para utilizar los diversos recursos: se da de alta en el dominio *Compras* cuando quiere utilizar la red propia y en el dominio *Ventas* cuando necesita datos de ventas; un procedimiento bastante pesado.

Para ello existe un truco: si las autorizaciones de acceso en ambos dominios coinciden (es decir, el nombre de usuario y la contraseña son iguales), el señor X puede utilizar los recursos compartidos para él del dominio *Ventas,* si está registrado en su propio dominio, *Compras*.

Las posiciones de confianza siempre son unilaterales: si, como en nuestro ejemplo, el dominio *Ventas* comparte recursos con miembros seleccionados del dominio *Compras*, no significa que el dominio *Ventas* pueda acceder a los recursos del dominio *Compras*. Para ello, este último también tendría que construir una posición de confianza.

6.5 Organizar dominios

Los dominios articulan las redes extensas en redes parciales más claras, y con ello reducen el trabajo de administración. Windows NT soporta hasta 26.000 usuarios y unos 250 grupos de dominio. Sin embargo, no es posible administrar tales cantidades de forma cómoda.

El número de dominios en que se divide una organización depende de:

el número de usuarios

la organización empresarial y

las necesidades en cuanto a seguridad de cada uno de los departamentos.

A continuación voy a presentar distintos modelos y sus posibilidades de aplicación.

Los límites del sistema

En primer lugar, el número de usuarios, de ordenadores y de grupos de usuarios influye en la división de una red Windows NT. Para su administración, Windows NT crea una base de datos denominada Directory Database. Esta puede alcanzar como máximo 40 Mbyte y se encuentra tanto en el controlador principal de dominio como en el controlador de dominio de reserva.

Windows NT necesita espacio disponible para cada elemento:

1 Kbyte para cada usuario

0,5 Kbytes para cada ordenador de la red y

4 Kbytes para un grupo de unos 300 usuarios.

Mediante estos números se pueden plantear situaciones sobre cuándo y con qué configuración una red traspasará los límites de Windows NT.

Un dominio único

La forma de organización más sencilla de una red NT es un dominio único. Los accesos de los usuarios y los recursos del dominio son controlados por un controlador principal de dominio (PDC) y uno o varios controladores de dominio de reserva (BDC). Cada controlador de dominio puede administrar hasta 5.000 usuarios si está equipado con la memoria RAM suficiente.

En un dominio único, los administradores del PDC (controlador principal de dominio) pueden gestionar todos los usuarios, todos los ordenadores (clientes y servidor) y todos los recursos del dominio. Esto requiere una administración eficaz. Si se divide la red, también se dividen las tareas administrativas en varias posiciones.

Dominios maestros únicos

Si una red es lo suficientemente pequeña para administrarse en un dominio único pero, por razones de organización, dentro de la empresa se necesitan distintos dominios, la opción apropiada es el concepto de dominios maestros únicos. En el mismo, todos los usuarios y grupos de usuarios globales se crean y administran en el domino maestro. Los ordenadores de cada una de las distintas unidades organizativas de la empresa se sitúan en distintos dominios, los cuales ponen su confianza en el dominio maestro.

En este modelo, los usuarios se registran en el domino maestro. Este dominio en sí no ofrece ningún otro recurso, sino que únicamente regula las configuraciones de seguridad de los usuarios y grupos de usuarios. Los recursos propiamente dichos son ofrecidos por los otros dominios. Gracias a la posición de confianza unilateral del resto de dominios hacia el dominio maestro, éste puede servir de mediador entre los recursos de cada uno de los dominios.

Un dominio maestro se administra de forma centralizada. Esta tarea se puede realizar por un centro de cálculo o un departamento especial de informática. En este caso, los administradores se benefician de la administración centralizada: deben cuidarse en un único dominio de los usuarios y grupos de usuarios, así como de sus configuraciones de seguridad y, por lo tanto, pueden administrar una red de muchos dominios distintos.

En cambio, los recursos de cada uno de los dominios de una red de este tipo pueden administrarse en el dominio maestro o en el dominio respectivo. Los datos delicados como la administración de usuarios se deja en unas manos, mientras que los datos menos delicados, como la administración de recursos, se delegan a cada una de las unidades organizativas que gestionan dominios propios. Cada uno de los dominios se puede dividir para adaptarse a la organización de la empresa.

En una organización de este tipo, los controladores de dominio de reserva de cada uno de los dominios trabajan como controladores de dominio de reserva del dominio maestro y aseguran la red múltiples veces contra fallos de los controladores de dominio.

Dominios maestros múltiples

En el caso de los dominios maestros múltiples, se vinculan entre si dos o más dominios maestros. Todos los dominios de los dominios maestros tienen una posición de confianza unilateral hacia todos los dominios maestros. Los dominios maestros, por su parte, tienen una posición de confianza bilateral entre sí. Al igual que en el concepto de dominios maestros únicos, los accesos de usuarios sólo se gestionan en los dominios maestros, mientras que el resto de dominios ponen a disposición sus recursos.

En un dominio maestro múltiple (dividido), cada usuario de cualquier dominio de recursos puede registrarse en cualquier dominio maestro, ya que los dominios maestros tienen posiciones de confianza bilaterales en ambas direcciones. En este modelo, a cada usuario del dominio maestro se le asigna exactamente una cuenta de ordenador, de forma que en cada dominio maestro se pueden administrar hasta 26.000 usuarios.

Organización flexible

Los dominios maestros múltiples ofrecen las siguientes ventajas:

Es posible administrar organizaciones con más de 40.000 usuarios dividiéndolas en distintos dominios maestros. En principio, el concepto de los dominios múltiples no tiene número máximo de usuarios, puesto que se pueden instalar tantos dominios maestros como se desee.

Los usuarios móviles, como colaboradores en el exterior, pueden conectarse desde cualquier lugar del mundo y desde cualquier dominio de recursos de la red.

La red se puede administrar de forma centralizada (dentro del marco de los dominios maestros) o descentralizada (también a nivel de los dominios de resursos).

En el modelo de dominios maestros múltiples también se pueden reproducir estructuras organizativas complejas. Las empresas con filiales por todo el mundo, las unen en una sola red a través de dominios maestros divididos. Dicha red se puede administrar, a pesar de todo, de forma centralizada dentro de cada una de las filiales.

Los controladores de dominio de reserva pueden estar distribuidos a través de LANs y WANs para protegerlas especialmente contra pérdidas de datos debidas a incendio o catástrofe similar.

6.6 Solución para los nombres

Con la red cliente−servidor y el concepto de dominios, podría estar solucionado el riesgo de seguridad de este concepto de red tan simple. Pero ahora queda por resolver la cuestión de los nombres: ¿cómo pueden saber los usuarios de una red, ya sea cliente−servidor o punto a punto, qué ordenador ha compartido qué recursos y con qué nombre?

Este problema lo solucionan distintos conceptos.

Listas de nombres estáticas

La solución más simple es un archivo con los nombres y los recursos compartidos de todos los clientes y servidores de la red. Consultando este archivo se pueden observar los recursos disponibles.

Un archivo de este tipo debe estar ubicado de forma centralizada en el servidor de registro de la red, a fin de que los clientes lo puedan consultar. El concepto es sencillo y suficiente, siempre y cuando no se modifique mucho la estructura de la red. Sobre todo no se debe modificar el nombre del servidor, ya que en tal caso los clientes ya no sabrían dónde se tienen que registrar y, por lo tanto, tampoco podrían consultar las listas de recursos. Además, no se conocen todos los recursos compartidos hasta que no se reinician los clientes y el servidor.

Estas listas de nombres estáticas también existen actualmente en Windows NT. Con ellas es posible administrar:

los nombres para el NetBIOS en el archivo *Lmhosts*

los nombres de redes TCP/IP en el archivo *Hosts.*

Ambos archivos se encuentran en el subdirectorio *System32Drivers\etc* del directorio raíz de Windows NT.

Listas dinámicas

Una ampliación sencilla del concepto son las listas dinámicas. Aquí, el servidor consulta los recursos compartidos en todos los ordenadores de la red, a intervalos regulares. De esta forma, los clientes también conocen, a intervalos regulares, los nuevos recursos compartidos del servidor. Este concepto representado en redes Novell 3.1x se denomina Service Advertising Protocol (SAP). El inconveniente decisivo de esta solución se presenta en redes grandes con numerosos recursos compartidos: en estos casos, la actualización de las listas sobrecarga la red.

Examinador de red

La primera respuesta de Microsoft a la problemática de los nombres consistió en los examinadores de red. Estos programas pueden examinar la red para buscar ordenadores disponibles y, dentro de cada uno de estos ordenadores, recursos compartidos. Como esta lista se crea de nuevo cada vez que se consulte, el concepto es particularmente aconsejable para redes punto a punto, en las cuales se pueden modificar a corto plazo los recursos disponibles. Como esta búsqueda en la red también debe ser organizada, en las redes Windows NT existe un examinador maestro, que suele ser el controlador principal de dominio, aunque no es necesario. Cada cliente, al darse de alta en el servidor también se da de alta en el examinador maestro con el mensaje de incluirse en la lista.

Pero también el concepto del examinador llega a sus límites en redes grandes. Si las listas de recursos disponibles son demasiado extensas, la consulta dura mucho tiempo. Es por ello que la consulta de recursos se ha restringido al grupo de trabajo o dominio en el que se ha dado de alta la cliente. Del resto de grupos de trabajo y dominios sólo se indican los nombres. En caso de que, incluso así, en redes grandes surjan problemas, es posible separar los dominios mediante tipologías de red *bridge* o *router*. Para ello, los dominios deben comportarse como subredes en un entorno TCP/IP.

Servidor de nombres

En redes realmente grandes, la relación de los nombres no puede realizarse mediante examinadores. En estos casos, cada ordenador debe tener una dirección única, a través de la cual se pueda consultar. De la asignación de los nombres de los ordenadores se encarga entonces el servidor de nombre. Estas máquinas contienen una base de datos sencilla que asigne nombres a las direcciones de los ordenadores. Si existen varios servidores de nombre, deben estar sincronizados entre sí. La dirección de un ordenador debe ser única en toda la red.

Esta vía es la que se aplica en Internet basada en TCP/IP. Desde el Service Pack 3 de la versión 3.51 de Windows NT, este programa puede actuar también como servidor de nombre. Antes de dicha versión únicamente había servidores WINS, que convertían los nombres y direcciones de redes Windows al sistema DNS y viceversa. Si dentro de una red Windows NT también se utiliza el protocolo TCP/IP, el servidor de nombre de Windows NT Server puede relacionar todos los nombres de esa red.

En los apartados siguientes describiré de forma breve (ya que no considero oportuno extenderse en un tema tan complejo, del cual derivarían hojas y hojas de información de muy difícil asimilación), los servicios DNS y WINS de Windows NT.

6.7 Los servicios WINS

La relación de nombres en Windows NT puede realizarse a través de dos vías distintas:

NetBIOS a través de TCP/IP (NetBT), el servicio WINS que describimos en este apartado y

DNS (Domain Name System), que presentamos en el apartado siguiente.

El servicio WINS forma parte de las capas de protocolo de la red Windows NT y convierte los nombres de los ordenadores de la red Windows en direcciones IP. Para ello, este servicio trabaja junto con el examinador de red, el cual relaciona los ordenadores registrados en la red.

6.8 Servicios DNS

El sistema jerárquico DNS (*Domain Name System*, Sistema de nombres de dominio) con una base de datos dividida, asigna nombres a los ordenadores en Internet. En principio, DNS trabaja como WINS: en una base de datos se asignan los nombres DNS a las direcciones únicas de cada ordenador. No obstante, a diferencia de WINS, DNS trabaja con una base de datos estática que tiene preparada esa información.

6.9 Instalar clientes

En redes basadas en el servidor, una de las principales tareas (que por cierto suele llevar bastante tiempo) del administrador del sistema es la instalación de clientes. En esta cuestión Windows NT puede prestar mucha ayuda. Con el administrador de clientes de red pueden crear disquetes de inicio y de instalación para clientes.

Con esta opción se crea un disquete de inicio que arranca el cliente y puede conectarlo inmediatamente con la red NT. Tras establecer la conexión se instala automáticamente el sistema seleccionado (Windows para trabajo en grupo o Windows NT Workstation) en el cliente. Para la instalación de Windows para trabajo en grupo es preciso que previamente se haya instalado un DOS en el cliente.

De esta forma, se pueden instalar clientes de todas las versiones de Windows y clientes de MS−DOS.

Para crear el disquete de inicio de cliente debe saber si el mismo arranca desde una unidad de 3 ½ o de 5 ¼ pulgadas (hoy en dia seria raro el segundo caso) y qué tarjeta de red está instalada en ese ordenador. Evidentemente, debe tratarse de una tarjeta compatible con Windows NT.

Si el cliente no debe ser instalado a través de la red, cree un juego de disquetes para instalar el cliente en el servidor. También puede utilizar la rutina de instalación de Windows para trabajo en grupo del CD−ROM del servidor NT.

De esa forma se crean disquetes de instalación para:

redes MS−DOS

LAN−Manager para MS−DOS y OS/2

redes RAS para MS−DOS y

TCP/IP para Windows 3.11.

No siempre el administrador del sistema puede trabajar directamente en el servidor NT para instalar un nuevo usuario u ordenador. Es por ello que se pueden compartir para determinados clientes, programas básicos de administración de redes en el servidor, en un directorio aparte. Las configuraciones deseadas se pueden realizar entonces a través de la red. Este procedimiento, no obstante, sólo se puede aplicar en Windows NT Workstation o en ordenadores Windows 95.

7 PROCESOS E HILOS

7.1 Procesos

Habitualmente, se define un proceso como un ejemplar de un programa en ejecución. Un proceso obviamente emplea espacio de memoria y además ciertos recursos adicionales, tales como archivos, porciones de memoria dinámica e hilos. Los diversos recursos creados durante la vida e un proceso de destruyen en el momento en que éste termina.

Los procesos son *inertes*. Para que un proceso lleve a cabo algo, debe poseer un hilo; es este hilo el responsable de la ejecución del código presente en el espacio de direcciones del proceso. De hecho, un proceso puede tener varios hilos ejecutando código en su espacio de direcciones simultáneamente. Para hacerlo posible, cada hilo tiene su propio conjunto de registros de la CPU y su propia pila. Cada proceso tiene

al menos un hilo que ejecuta código en el espacio de direcciones del proceso. En el caso de que no exista ningún hilo que ejecute código en el espacio de direcciones del proceso, no hay razón para que este último siga existiendo, por lo que el sistema lo destruye a él y a su espacio de direcciones.

Para que se ejecuten todos esos hilos, el sistema operativo planifica y distribuye el tiempo de la CPU entre ellos. El sistema operativo crea la ilusión de que todos los hilos se ejecutan simultáneamente entregándoles rodajas de tiempo (*time slice*) de modo cíclico.

Cada proceso tiene un bloque de entorno asociado. Un bloque de entorno consiste en un bloque de memoria reservada dentro del espacio de direcciones del proceso. Cada bloque contiene un conjunto de cadenas con el siguiente aspecto:

NombreVar1=ValorVar1\0

NombreVar2=ValorVar2\0

NombreVar3=ValorVar3\0

....

NombreVarX=ValorVarX\0

La primera parte de cada cadena es el nombre de una variable de entorno. En nombre va seguido del signo igual, al que sigue el valor que se desea asignar a la variable. Todas las cadenas del bloque de entorno deben estar ordenadas alfabéticamente, en función de los nombres de las variables.

A causa de la utilización del signo igual para separar el nombre del valor, dicho signo no puede formar parte del nombre. Además, los espacios son significativos. Por ejemplo, si se declaran dos variables:

XYZ= Win32 {Obsérvese el espacio que sigue al signo igual.}

ABC=Win32

Y a continuación se comparan los valores de XYZ y ABC, el sistema informará que son diferentes.

Normalmente, un proceso hijo hereda un conjunto de variables de entorno que coincide exactamente con el de su proceso padre. Sin embargo, el proceso padre puede controlar qué variables de entorno va a heredar el proceso hijo. Cuando digo heredar, quiero decir que el proceso hijo obtiene su propia copia del bloque de entorno del padre, no que ambos comparten el mismo bloque. Esto significa que el proceso hijo puede añadir, borrar o modificar variables en su bloque, y estos cambios no se reflejan en el bloque del padre.

Habitualmente, las aplicaciones utilizan las variables de entorno para dar la oportunidad al usuario de hacer ajustes finos del comportamiento de las mismas. El usuario crea una variable de entorno y le asigna su valor. Entonces, cuando el usuario invoca la aplicación, ésta examina el bloque de entorno buscando la variable. Si la encuentra, la aplicación analiza su valor y ajusta su comportamiento.

El problema es que los usuarios no suelen entender ni asignar valor a las variables de entorno con facilidad. Los usuarios deben deletrear correctamente los nombres de las variables, y también deben conocer con exactitud la sintaxis que la aplicación espera en los valores. Por otra parte, la mayoría (si no todas) de las aplicaciones gráficas permitan a los usuarios realizar el ajuste fino del comportamiento de las mismas mediante cuadros de dialogo. Esta aproximación es mucho más amigable para el usuario, y también es más recomendable.

Cada proceso tiene asociado un conjunto de banderas que indican al sistema cómo debería responder el proceso ante errores serios. Entre los errores serios están los fallos del medio de almacenamiento de los discos, escepciones sin gestión prevista, fracasos en la búsqueda de archivos, y un mal alineamiento de los datos. Un proceso puede indicar al sistema cómo gestionar cada uno de estos errores si llama a la función *SetErrorMode:*

UINT *SetErrorMode* (UINT *fuErrorMode*);

El parametro *fuErrorMode* es una combinación de cualquiera de las banderas de la tabla adjunta, realizando una operación OR lógica a nivel de bit con las mismas.

Bandera	**Descripción**
SEM_FAILCRITICALEERRORS	El sistema no muestra el cuadro de mensajes del gestor de errores críticos y devuelve el tipo de error al proceso que hizo la llamada.
SEM_NOGPFAULTERRORBOX	El sistema no muestra el cuadro de mensajes de fallo de protección general (PG). Esta bandera sólo debe ser activada por aplicaciones de depuración que son capaces de tratar los fallos de PG por sí mismas, con un gestor de excepciones.
SEM_NOOPENFILEERRORBOX	El sistema no muestra un cuadro de mensajes cuando fracasa al tratar de encontrar un archivo.
SEM_NOALIGNMENTFAULTEXCEPT	El sistema corrige automáticamente los alineamientos de memoria defectuosos y los hace invisibles a la aplicación. Esta bandera no tiene efecto en los procesadores *x*86 o Alpha.

Por omisión, un proceso hijo hereda las banderas de modo de error de su padre. En otras palabras, su un proceso tiene en la actualidad activada la bandera SEM_NOGPFAULTERRORBOX y engendra un proceso hijo, éste tendrá también dicha bandera activada. Sin embargo, esto no se le notifica al proceso hijo, y quizá no haya sido escrito para que gestione los errores por fallo de PG. Si ocurriera un fallo de PG en uno de los hilos del proceso hijo, la aplicación hija podría concluir sin avisar al usuario. De todas formas, un proceso padre puede evitar que su modo de error sea heredado por sus hijos.

Un proceso puede terminar de tres maneras:

Un hilo del proceso llama a la función *ExitProcess* (éste es el método más común).

Un hilo de otro proceso llama a la función *TerminateProcess* (este método debe evitarse).

Todos los hilos del proceso se mueren por sí solos (esto rara vez ocurre).

Procesos hijos

Cuando se diseña una aplicación, surgen situaciones en las cuales se desea que otro bloque de código lleve a cabo un determinado trabajo. A menudo se asigna el trabajo mediante llamadas a funciones o subrutinas. Cuando se llama a una función, la ejecución del código que la llama queda detenida hasta que esta vuelve. Y en muchas situaciones, s necesaria esta sincronización de una única tarea.

Una manera alternativa para que otro bloque de código lleve a cabo una tarea es crear un nuevo hilo en el proceso y hacer que colabore en el procesamiento. Esto permite al código restante continuar la ejecución

mientras el hilo lleva a cabo el trabajo solicitado. Esta técnica es útil, pero crea problemas de sincronización cuando el hilo original desea ver los resultados obtenidos por el nuevo hilo.

Otra aproximación es la de engendrar un nuevo proceso −in proceso hijo− para que eche una mano con el trabajo. Supongamos que el trabajo a realizar es bastante complejo. Para acometerlo, simplemente se decide crear un nuevo hilo en el proceso. Se escribe el código correspondiente, se prueba y se observan resultados incorrectos. Podría haber un error en el algoritmo, o quizá se desreferenció algo de manera incorrecta, produciendo la sobreescritura de alguna cosa importante en el espacio de direcciones. Una forma de proteger el espacio de direcciones y conseguir que se haga el trabajo es crear un nuevo proceso que se ocupe de ello.

7.2 Hilos

Un hilo describe una trayectoria de ejecución dentro de un proceso. Cada vez que arranca un proceso, el sistema crea su hilo principal. Para muchas aplicaciones, este hilo principal es el único que requieren. Sin embargo, los procesos pueden crear hilos adicionales que les ayuden en su trabajo. La idea que subyace a todo esto es la de aprovechar todo el tiempo de CPU que sea posible.

Por ejemplo, un programa de hoja de cálculo necesita recalcular los resultados a medida que el usuario modifica los datos introducidos en las celdas. Dado que esos cálculos le pueden llevar varios segundos si la hoja de cálculo es compleja, una aplicación bien diseñada no recalcula todo cada vez que el usuario hace un cambio. En vez de esto, la función para recalcular se ejecuta en un hilo aparte, de menor prioridad que el hilo principal. Así, el usuario está tecleando, se ejecuta el hilo principal, lo que significa que el sistema no planificará tiempo para el hilo que recalcula la hoja. Cuando el usuario deja de teclear, el hilo principal se para, esperando nueva entrada, y se asigna el tiempo al segundo hilo. Tan pronto como el usuario vuelve a teclear, el hilo principal, que tiene mayor prioridad, apropia la CPU al hilo que recalcula. Al crear un hilo adicional, el programa responde al usuario de una manera mucho más rápida. Además, es bastante sencillo implementar este tipo de diseño.

Cuando no se debe crear un hilo

A muchos programadores les ocurre que, la primera vez que se les da acceso a un sistema que admite múltiples hilo, entran en éxtasis. Si hubieran podido tener hilos antes, sus aplicaciones habrían sido tan sencillas de escribir... Y, por alguna razón desconocida, estos programadores empiezan a dividir una aplicación en trozos, cada uno de los cuales se puede ejecutar en un hilo. Ésta no es la manera correcta de proceder a la hora de desarrollar una aplicación.

Los hilos son increíblemente útiles, y tienen su lugar, pero al utilizar hilos se pueden crear nuevos problemas potenciales al intentar resolver los antiguos. Por ejemplo, digamos que estamos desarrollando una aplicación de proceso de texto y deseamos permitir a la función de impresión que se ejecute en su propio hilo. Esto suena bien, ya que de ese modo el usuario podrá volver a editar el documento de inmediato, mientras éste se está imprimiendo. Pero, un momento: esto significa que los datos del documento podrían cambiar durante la impresión. Esto hace surgir un nuevo tipo de problema enteramente nuevo, que será necesario acometer. Quizá no fuera lo mejor tener la impresión ejecutándose en su propio hilo; pero esta solución parece un tanto drástica. ¿Qué tal si permitimos al usuario que edite otro documento, mientras el que se imprime queda bloqueado hasta que concluya la impresión? O copiar el documento a un archivo temporal, imprimir el contenido del archivo temporal y dejar que mientras el usuario modifique el original. Una vez que ha concluido la impresión del archivo temporal, éste puede borrarse.

Como se puede ver, los hilos ayudan a solucionar algunos problemas pero de corre el riesgo de crear otros nuevos.

Al igual que un proceso, el hilo puede terminar de tres maneras:

El hilo se suicida llamando a la función *ExitThread* (el método más común).

Un hilo del mismo procedo, o de otro, llama a *TerminateThread* (método a evitar).

Termina el proceso al que pertenece el hilo.

Como planifica los hilos el sistema

Un sistema operativo debe utilizar algún algoritmo para planificar cuándo se ejecutará cada hilo y durante cuánto tiempo.

Este apartado describe a grandes rasgos el algoritmo empleado por los sistemas operativos de Win32 para la planificación de hilos. Es necesario aclarar que Microsoft se reserva el derecho de modificar el algoritmo sutilmente. De hecho, ha ejercido este derecho, de modo que los algoritmos de Windows 95, Windows NT3.5 y Windows NT 4 son ligeramente distintos. Microsoft altera el algoritmo cuando considera que las aplicaciones rendirán más tras la modificación. La información que se presenta a continuación debe considerarse como líneas generales, teniendo en cuenta que algunas cosas pueden cambiar a medida que pase el tiempo.

El sistema planifica la ejecución de cada hilo activo en función de su nivel de prioridad. En el sistema, se asigna un nivel de prioridad a cada hilo. El rango de los niveles de prioridad va desde 0, el mínimo, hasta 31, el máximo. El nivel de prioridad 0 se asigna a un hilo especial del sistema denominado hilo de la *página cero*. El hilo de la página cero es responsable de poner a cero todas las páginas de estén libres en el sistema, mientras que no haya otros hilos que deban desempeñar algún trabajo. Ningún otro hilo puede tener un nivel de prioridad de 0.

A la hora de signar una CPU a un hilo, el sistema trata por igual a todos los hilos de la misma prioridad; esto quiere decir que, el sistema simplemente asigna el primer hilo de prioridad 31 a una CPU, y una vez ha concluido su *time slice*, asigna la CPU al siguiente hilo de prioridad 31. Una vez que todos los hilos de prioridad 31 han dispuesto de su rodaja de tiempo, el sistema vuelve a asignar la CPU al primero de ellos. Nótese que, si siempre se dispone de hilos de prioridad 31 para cada CPU, otros hilos con prioridad menor que 31 nunca podrían asignarse a ninguna CPU, por lo que nunca se ejecutarían. Esta condición se denomina *inanición*. La inanición ocurre cuando hay hilos que consumen tal cantidad de tiempo de la CPU que otros hilos no tienen oportunidad de ejecutarse nunca.

Una vez que no quedan hilos de prioridad 31 pendientes de ejecutarse, el sistema comienza a asignar la CPU a los hilos de prioridad 30. Cuando ya no haya hilos de prioridades 31 ni 30 con necesidad de ejecutarse, el sistema asigna la CPU a los hilos de prioridad 29, y así sucesivamente.

De entrada, podría pensarse que los hilos de baja prioridad (como el hilo de la página cero) nunca tendrían posibilidad de ejecutarse en un sistema diseñado de este modo. Pero se hace patente que, con frecuencia, los hilos no tienen ninguna razón para ejecutarse. Por ejemplo, si el hilo principal de un cierto proceso llama al *GetMessage*, y el sistema ve que no hay mensajes pendientes, detiene la ejecución del hilo, apropia lo que queda de la rodaja de tiempo y asigna la CPU a otro hilo en espera.

Si no aparecen mensajes que deba recuperar *GetMessage*, el hilo del proceso permanece detenido y nunca se le asigna la CPU. Sin embargo, si entra algún mensaje en la cola de ese hilo, el sistema se percata de que ya no debe permanecer detenido, y le asignará la CPU en el momento en que no haya hilos de mayor prioridad con necesidad de ejecutarse.

También quiero apuntar otra cuestión. Si está en ejecución un hilo de prioridad 5, y el sistema determina que un hilo de mayor prioridad está preparado para su ejecución, el sistema detiene de inmediato el hilo de menor

prioridad (aunque esté en medio de su *time slice*) y asigna la CPU al hilo de mayor prioridad, que obtiene una rodaje de tiempo completa. Los hilos de mayor prioridad siempre apropian la CPU a los de menor prioridad, con independencia de lo que estés ejecutando estos últimos.

Cómo se asignan los niveles de prioridad mediante la API Win32

Cuando se crean hilos, no se les asigna su nivel de prioridad con números. En lugar de esto, el sistema determina el nivel de prioridad del hilo en un proceso de dos pasos. El primer paso consiste en asignar una clase de prioridad al proceso. La clase de prioridad del proceso indica al sistema la prioridad que tiene el proceso en comparación con la de los que estén en ejecución. El segundo paso es asignar prioridades relativas a los distintos hilos que posea el proceso. Los siguientes puntos describen ambos pasos.

Clases de prioridad de proceso

Win32 admite cuatro clases de prioridad distintas: en reposo, normal, lata y de tiempo real. Se asigna una clase de prioridad al proceso haciendo un OR lógico de una de las banderas que se muestran en la siguiente tabla con las restantes banderas de *fdwCreate*, en la llamada a *CreateProcess*. En esta tabla se muestra el nivel de prioridad asociado a cada una de las clases:

Clase	**Bandera de CreateProcess**	**Nivel**
En reposo	IDLE_PRIORITY_CLASS	4
Normal	NORMAL_PRIORITY_CLASS	8
Alta	HIGH_PRIORITY_CLASS	13
De tiempo real	REALTIME_PRIORITY_CLASS	24

Esto significa que cualquier hilo que se cree en un proceso cuya clase de prioridad es normal, tiene el nivel de prioridad 8.

Nunca insistiremos lo suficiente en lo necesario que resulta hacer con cuidado la elección de la clase de prioridad de un proceso. Al llamar a *CreateProcess*, la mayoría de las aplicaciones deberían, o bien no indicar la clase de prioridad, o bien utilizar la bandera NORMAL_PRIORITY_CLASS. Si no se especifica la clase de prioridad el sistema asume que esta será la normal, a menos, que el proceso padre pertenezca a la clase en reposo. En este caso, el proceso hijo también pertenecerá a esa clase.

Los procesos de la clase de prioridad normal se comportan de una manera ligeramente distinta de cómo lo hacen los de otras clases de prioridad. La mayoría de las aplicaciones que ejecuta un usuario son de la clase de prioridad normal. Por otra parte, si el usuario trabaja con un proceso dado, ese proceso se denomina proceso en primer plano, mientras que los restantes se denominan procesos en segundo plano.

En Windows NT, cuando un proceso normal pasa al primer plano, el sistema incrementa el cuanto de tiempo que se otorga a cada uno de los hilos que se ejecuten dentro del proceso. Por ejemplo, supongamos que a los hilos se les asigna un cuanto de 15 milisegundos cada vez que se planifican. Sin embargo, cuando el sistema planifica un hilo que está ejecutándose en un proceso normal de primer plano, incrementa el cuanto de tiempo del hilo en un factor de 3, de manera que el hilo recibe un cuanto de tiempo de 45 milisegundos.

La razón de ser de estos cambios a los procesos en primer plano es conseguir que reaccionen más rápido a la entrada del usuario. Si no se hicieran cambios en los hilos del proceso, un proceso normal de impresión en segundo plano y un proceso normal que aceptara entrada por parte del usuario en primer plano estarían compitiendo por el tiempo de la CPU en igualdad de condiciones. El usuario apreciaría, que el texto no surgiría con fluidez en su aplicación de primer plano. Pero dado que el sistema altera los hilos de los procesos situados en primer plano, éstos procesan la entrada del usuario de una manera más dinámica.

Con Windows NT, el usuario puede controlar la mejora de prestaciones que hace el sistema en los procesos normales de primer plano, pulsando dos veces en la opción Sistema del *Panel de Control*, y después pulsando en la etiqueta *Rendimiento*. Ésta presenta un cuadro de diálogo, donde la barra de desplazamiento *Mejora* indica en qué medida debe mejorarse el cuanto de tiempo de los hilos de primer plano. Si la barra de desplazamiento está en *Ninguno*, el cuanto del hilo se multiplica por 1; si la barra de desplazamiento está en *Máximo* el cuanto de tiempo se multiplica por tres; y si está en el medio, el cuanto se multiplica por 2.

La prioridad en reposo es perfecta para aplicaciones que vigilen el sistema. Por ejemplo, podría escribirse una aplicación que muestre periódicamente la cantidad de RAM disponible en el sistema. Como no sería deseable que esta aplicación interfiriera en las prestaciones de otras aplicaciones, habría que establecer que la clase de prioridad de este proceso fuera IDLE_PRIORITY_CLASS.

Otro buen ejemplo de una aplicación que puede utilizar la prioridad en reposo es un protector de pantallas. Un protector de pantallas pasa la mayor parte del tiempo simplemente observando las acciones del usuario. Cuando el usuario permanece inactivo, durante un cierto periodo de tiempo, el protector de pantallas se activa. No hay razón para que el protector de pantallas observe las acciones del usuario con alta prioridad, así que su prioridad puede ser perfectamente en reposo.

La clase de alta prioridad sólo debe utilizarse cuando resulte absolutamente necesario.

La cuarta bandera de prioridad, REALTIME_PRIORITY_CLASS, no debe utilizarse prácticamente nunca. La prioridad de tiempo real es extremadamente alta, y dado que la mayoría de los hilos en el sistema (incluidos los de gestión del sistema) se ejecutan con una prioridad menor, se verían afectados por un proceso de esta clase. En la práctica, los hilos del sistema que controlan el ratón y el teclado, el volcado a disco en segundo plano, y la vigilancia de la combinación Ctrl+Alt+Del, operan todos ellos con una prioridad menor que la de la clase de tiempo real. Si el usuario está moviendo el ratón, el hilo que controla su movimiento pierde la CPU ante la llegada de un hilo de tiempo real. Esto afecta al movimiento del ratón, que se moverá a trompicones, en vez de hacerlo con suavidad. Pueden también, presentarse consecuencias más serias que ésta, como pérdidas de datos.

Podría utilizarse la clase de prioridad de tiempo real si se escribe una aplicación que se entienda directamente con el hardware, o si se necesita realizar alguna tarea de corta duración y se quiere tener una seguridad casi absoluta de que no va a ser interrumpida.

Un proceso no puede ejecutarse con la clase de prioridad de tiempo real si el usuario que ha accedido al sistema no dispone del privilegio de Incremento de la prioridad en la planificación. Cualquier usuario que se designe como administrador o bien como usuario intensivo tiene este privilegio por defecto. Se puede otorgar este privilegio a otros usuarios o grupos de usuarios mediante el Administrador de usuarios de Windows NT.

Como establecer la prioridad relativa de un hilo

Cuando se crea un inicialmente un hilo, su nivel de prioridad es el de la clase de prioridad de su proceso. Por ejemplo, al hilo principal de un proceso de la HIGH_PRIORITY_CLASS se le asigna un nivel de prioridad inicial de 13. A pesar de ello, es posible elevar o disminuir la prioridad de los hilos individuales. La prioridad de un hilo está siempre relacionada con la clase de prioridad del proceso que lo posee.

Se puede cambiar la prioridad relativa dentro de un proceso de un hilo del mismo llamando a *SetThreadPriority:*

BOOL SetThreadPriority (HANDLE hThread, int nPriority);

El primer parámetro, *hThread*, es el descriptor del hilo cuya prioridad se desea modificar. El parámetro

nPriority puede ser cualquiera de los valores que se muestran en la tabla siguiente.

Identificador	**Significado**
THREAD_PRIORITY_LOWEST	La prioridad del hilo debe ser dos unidades menor que la de la clase del proceso.
THREAD_PRIORITY_BELOW_NORMAL	La prioridad del hilo debe ser una unidad menor que la de la clase del proceso.
THREAD_PRIORITY_NORMAL	La prioridad del hilo debe ser igual que la de la clase del proceso.
THREAD_PRIORITY_ABOVE_NORMAL	La prioridad del hilo debe ser una unidad mayor que la de la clase del proceso.
THREAD_PRIORITY_HIGHESTLOWEST	La prioridad del hilo debe ser dos unidades mayor que la de la clase del proceso.

En el momento de crear un hilo, su prioridad inicial es THREAD_PRIO−RITY_NORMAL. Las reglas que se aplican a los hilos dentro de los procesos son similares a las que se aplican a los hilos de diferentes procesos. Sólo se debe asignar a un hilo la THREAD_PRIORITY_HIHGEST cuando sea absolutamente necesario para que el hilo se ejecute correctamente. El planificador dejará morir de inanición a los hilos de menor prioridad si hay hilos de alta prioridad que necesiten ejecutarse.

Además de las banderas que recoge la tabla, se pueden pasar dos banderas especiales a *SetThreadPriority*: THREAD_PRIORITY_IDLE y THREAD_PRIORITY_TIME_ CRITICAL. Si se especifica THREAD_PRIORITY_IDLE, el nivel de prioridad del hilo se establece a 1, con independencia de que la clase de prioridad del proceso sea en reposo, normal o alta. Sin embargo, si la clase del proceso es de tiempo real, entonces el valor se establece en 16. Si se indica THREAD_PRIORITY_TIME_CRITICAL la prioridad del hilo se establece en 15, con independencia de que la clase del proceso sea en reposo, normal, o alta. Sin embargo, si la clase de prioridad del proceso es de tiempo real, THREAD_PRIORITY_TIME_CRITICAL establece el nivel de prioridad en 31. La siguiente tabla muestra el modo en que el sistema combina la clase de prioridad de un proceso con la propiedad relativa de los hilos, para calcular el nivel básico de prioridad de éstos.

Clases de prioridad del proceso

Prioridad relativa del hilo En reposo Normal Alta De tiempo real

Crítica en tiempo 15 15 15 31

La más alta 6 10 15 26

Superior a lo normal 5 9 14 25

Normal 4 8 13 24

Inferior a lo normal 3 7 12 23

La más baja 2 6 11 22

En reposo 1 1 1 16

Modo en que el sistema determina el nivel básico de prioridad de un hilo.

La tabla anterior muestra las prioridades de los hilos de los procesos de la clase normal, cuando se ejecutan en segundo plano. En Windows NT, estas prioridades no cambian al pasar el proceso al primer plano; sólo cambian los cuantos de tiempo que se asignan a los hilos.

Mejora dinámica de los niveles de prioridad de los hilos

El nivel de prioridad que se determina por la combinación de la clase de prioridad del proceso y la prioridad relativa del hilo se denomina *nivel básico de prioridad.* Ocasionalmente, el sistema mejora el nivel de prioridad de un hilo. Esto ocurre habitualmente como respuesta a la aparición de un suceso de E/S, tal como un mensaje de ventanas o una lectura de disco. Por ejemplo, un hilo con una prioridad relativa normal que se ejecute en un proceso de la clase de alta prioridad tiene un prioridad básica de 13.

Si el usuario pulsa una tecla, el sistema coloca un mensaje WM_KEYDOWS en la cola del hilo. A causa de que el mensaje aparezca en la cola del hilo, el sistema asigna temporalmente la CPU a ese hilo, para que pueda procesar el mensaje. Además, el sistema también hace una mejora temporal de la prioridad del hilo, desde 13 a 15 (el valor real puede variar). Este nuevo nivel de prioridad del hilo se denomina *prioridad dinámica*. Una vez que la CPU ejecuta el hilo durante una rodaja de tiempo completa, su prioridad baja a 14. De nuevo, cuando se le asigne la CPU y pueda ejecutar otra rodaja de tiempo completa, cuando ésta acaba, el sistema reduce de nuevo la prioridad en uno. El sistema no permite que la prioridad dinámica de un hilo nunca esté por debajo de su nivel básico de prioridad.

Microsoft hace continuamente ajustes finos de las mejoras dinámicas del sistema para alcanzar los mejores resultados medios. Todo este esfuerzo esta destinado a conseguir que el sistema responda de manera inmediata al usuario final. Dicho sea de paso, el sistema nunca mejora la prioridad dinámica de los hilos que están en el rango de tiempo real (valores de 16 a 31). El sistema sólo mejora los hilos del rango dinámico. Por otra parte, el sistema tampoco mejorará un hilo si su prioridad va a entrar en el rango de tiempo real (valores de 15 o superiores).

8 ADMINISTRACIÓN DE USUARIOS

Windows NT es un auténtico sistema operativo de red multiusuario. Por eso, a diferencia de Windows 95 y de Windows 3.x, es necesaria una administración de los usuarios. Los administradores del sistema son los que definen quién está autorizado a utilizar los dominios del servidor NT y con qué derechos. A los usuarios locales de NT Workstation se les ofrece la posibilidad de personalizar la pantalla de presentación del entorno Windows NT.

La administración de los usuarios tiene tareas fundamentales:

Posibilitar la personalización y optimización de la pantalla de presentación y el funcionamiento del sistema operativo para el mayor número de usuarios posible, de acuerdo con las necesidades de cada uno de ellos. Eso significa que, para proteger los datos, aveces es conveniente no permitir el libre acceso de todos los usuarios a todos los archivos de NT Server.

la segunda tarea fundamental es garantizar la seguridad del sistema. Los derechos limitados de todo usuario normal no permitan modificar los archivos más importantes del sistema (como son los archivos de registro) ni, por lo tanto, causar daños graves. Por esa razón no siempre es conveniente hacerse administrador de NT Workstation cuando se es el único usuario de la misma. Los administradores de red de un dominio NT sólo deberían entrar en la red como administradores para trabajos de mantenimiento: para reconocer rápidamente el mal uso de los derechos de acceso a la red de los usuarios normales.

La tercera tarea también está relacionada con la seguridad del sistema. Se trata, esta vez, de protegerse contra el acceso indebido de terceros. Si todos los usuarios aseguran sus derechos de acceso con contraseñas seguras, el acceso indebido de terceros a NT Server, una red Windows NT, o a Windows NT Workstation resulta mucho más difícil. La seguridad de Windows NT está sujeta a normas estrictas dictadas por el departamento de defensa de EE.UU. si bien en Windows NT se puede configurar un nivel de seguridad *Class C2*, en la práctica no tiene mucho sentido trabajar con este sistema debido a los constantes controles de seguridad y los protocolos de eventos. Windows NT Server debería quedar cerrado de manera mecánica, pues quien puede acceder físicamente a Windows NT Server, también puede manipular los datos guardados en él.

8.1 Panorámica

En Windows NT, la administración de usuarios se realiza a través del Administrador de usuarios y otros programas del sistema.

Utilice:

el *Administrador de usuarios para dominios* para crear nuevos usuarios, grupos locales y globales, definir directivas generales y crear un perfil y un *script* de conexión para cada uno de ellos.

el *Administrador de servidores* para definir las propiedades y derechos de acceso de los directorios libres del servidor, separar los usuarios del servidor NT o configurar la duplicación de directorios, y

el Explorador de Windows NT para realizar las configuraciones de seguridad de directorios y archivos o compartir recursos.

Con estas tres utilidades gráficas, se pueden crear y mantener usuarios y administrar los derechos de acceso y recursos del sistema.

8.2 El administrador de usuarios

Las personas administradoras de sistemas operativos gráficos como Windows NT necesitan una administración de usuarios que sea clara y economice trabajo. Y eso es precisamente lo que les ofrece el programa Administrador de usuarios para dominios. En las redes NT, los dominios son grupos de ordenadores regidos por las mismas directivas de seguridad y de información de cuentas (de los usuarios).

Estos datos están administrados y controlados por los Controladores de dominio: el controlador principal de dominio y el controlador secundario de dominio. La base de datos de usuarios NT se encuentra en el Controlador principal de dominio(PDC) y existe un duplicado de la misma en los restantes controladores de seguridad de dominio (BDC). Cuando falta el Controlador principal de dominio, el control de la inscripción de usuarios lo realiza el siguiente controlador de seguridad de dominio disponible.

El administrador de usuarios permite:

Crear usuarios, crear perfiles de usuario y llevar el mantenimiento de ambos

configurar información de cuentas para los usuarios

crear las propias cuentas

crear grupos

crear configuraciones de acceso (Logon)

realizar configuraciones de seguridad y

definir las relaciones de confianza para otros dominios.

Naturalmente, el *Administrador de usuarios* también posee sus propios derechos de acceso. Los administradores son los únicos autorizados a configurar todos los parámetros. Otras cuentas de usuario, como son el *operador de cuentas* o los *administradores de dominio* sólo están autorizados a configurar determinados parámetros del *Administrador de usuarios.*

8.3 Grupos de usuarios

Los grupos de usuarios reúnen varios usuarios en una unidad. Windows NT predetermina los grupos cuyas propiedades no se pueden modificar. Los grupos de usuarios se pueden crear en un solo dominio o bien en varios dominios enlazados entre sí por relaciones de confianza.

Con los grupos de usuario se pueden incorporar usuarios de un dominio a otro, siempre que los dominios hayan establecido una relación de confianza entre sí. De ese modo, los usuarios de los otros dominios no sólo pueden acceder a los recursos del otro servidor, sino incluso ser administrados por este.

Grupos de usuarios globales y locales

La creación de grupos de usuarios facilita enormemente la tarea de los administradores de la red. En lugar de definir detalladamente los derechos de acceso a la red para cada uno de los usuarios, los grupos permiten asignar los derechos en bloque a todo un grupo, ya sea predefinido o de creación propia. De ese modo, se otorgan diferentes derechos en una sola asignación.

Microsoft distingue entre grupos locales y grupos globales.

Los grupos globales están formados por diferentes usuarios del mismo dominio, agrupados con un solo nombre común. Los grupos de usuarios globales se crean dentro de un dominio y no pueden incluir usuarios de otros dominios. En compensación, a los grupos de usuarios globales, sí se les pueden asignar derechos en otros dominios. Por eso reciben estos grupos el calificativo de globales.

Los grupos locales están formados por usuarios y grupos globales. Estos grupos y usuarios pueden pertenecer indistintamente al dominio en que se ha creado el grupo local o a cualquier otro dominio de confianza.

A continuación explicaré mediante un ejemplo el porque de esta diferencia.

Imaginémonos una red sencilla Windows NT con los dominios COMPRAS y VENTAS. Se quiere que los usuarios de estos dominios puedan utilizar indistintamente los recursos del otro dominio. Para ello hay que crear, en primer lugar, una relación de confianza entre los dos dominios. Después se incluye el grupo Usuarios del dominio VENTAS en el grupo Usuarios del dominio COMPRAS. Ahora ya pueden acceder todos los usuarios de la red Ventas a los recursos de la red Compras. Para que los usuarios de Compras también pudiera acceder a la red VENTAS, se podría realizar la misma operación a la inversa, incluyendo el grupo Usuarios del dominio COMPRAS entre los usuarios del dominio VENTAS.

Con este segundo paso, sin embargo, se habría establecido una relación circular entre ambos grupos: COMPRAS sería una parte de VENTAS y VENTAS sería una parte de COMPRAS. Pero, ¿Quién sería entonces quién?

Para evitar este problema, se crearon los grupos de usuarios locales y globales. Si se incluye el grupo global Usuarios del dominio VENTAS en el grupo de usuarios local Compras, ambos grupos se pueden administrar

desde COMPRAS y ambos grupos pueden acceder indistintamente a los recursos libres del otro grupo.

Si administra grupos de usuarios en redes Windows NT con varios dominios, y los usuarios de cada dominio deben tener acceso a los recursos de los otros dominios, la manera de proceder más efectiva es la siguiente: forme un grupo local y un grupo global para cada recurso, por ejemplo: Administradores (local) y Administradores del dominio (global), Usuarios (local) y Usuarios del dominio (global).

Lleve el mantenimiento de los usuarios siempre en los grupos globales, pero incorpórelos a la vez en los grupos locales. De ese modo tendrá una administración de grupos local para cada uno de los dominios pudiendo incluir esos mismos usuarios en cualquier grupo local de todos los demás dominios con los que tenga establecida una relación de confianza. En general puede decirse que con los grupos globales se administran personas y con los grupos locales se administran recursos (por ejemplo, datos y programas).

Grupos de usuarios predefinidos

Para que se haga una idea clara de cómo y porqué Windows NT crea grupos de usuarios, se ha elaborado la siguiente lista con todas las propiedades de los grupos de usuarios predefinidos.

Administradores

Los administradores son, naturalmente quienes poseen la mayoría de los derechos para configurar los parámetros del servidor y de los dominios. La cuenta de administrador, como tal, no se puede borrar. Sólo se pueden borrar los administradores de dominio. Si bien los administradores poseen derechos plenos, su cuenta puede caducar. Por eso es aconsejable crear otras cuentas de administrador, como medida de seguridad, para poder recurrir a ellas en caso necesario (¡ imagínese, por ejemplo, qué pasaría si cambia la palabra clave de la cuenta de administrador y al cabo de unos días no se acuerda ya de ella ¡). Determinados archivos pueden estar bloqueados también para los administradores. Cada administrador puede conseguir acceso a todos los archivos, pero para esta acción debe seguir un protocolo; el auténtico usuario pierde así el acceso al archivo, lo cual le informa, indirectamente, de que el administrador ha tomado ese derecho.

Operadores de servidores

Este grupo posee todos los derechos para administrar un servidor de dominio. Puede liberar y bloquear recursos, realizar copias de seguridad y administrar usuarios. Los operadores de servidor pueden reiniciar el servidor de una red. Pero el operador no puede modificar el sistema del servidor. Los operadores del sistema son un grupo local.

Operadores de cuentas

Los operadores de cuentas pueden administrar los usuarios de un dominio y crear y mantener las cuentas de usuario. Sin embargo, hay determinadas cuentas especiales, como las de administradores y otros operadores, a las cuales no pueden acceder. De otro modo, los administradores de cuentas podrían convertirse por cuenta propia en administradores.

Operadores de impresión

Como su nombre indica, estos operadores se encargan única y exclusivamente de administrar los trabajos de impresión, sin poseer otros derechos especiales de acceso.

Operadores de copia

Los operadores de copias de seguridad pueden realizar copias de seguridad de los archivos del servidor, y de

las unidades de libre acceso de los clientes de la red NT, con la utilidad *Backup* de Windows NT u otro tipo de programa apropiado. No están autorizados a reproducir las copias de seguridad.

Duplicadores

Windows NT Server puede sincronizar sus directorios con otro equipo Windows NT Server o Workstation de la red. Al hacerlo, Windows NT Server está operando como servidor de exportación, los otros ordenadores de Windows NT son quienes importan los datos. De ese modo, se pueden hacer copias de seguridad de datos importantes en varios ordenadores a la vez, y administrar de manera central los directorios utilizados y modificados con mayor frecuencia, al mismo tiempo que se mantienen de manera local en los ordenadores. Para administrar esta función existe un grupo especial de usuarios: los *Duplicadores*. Por motivos de seguridad, ningún usuario estándar debería formar parte del grupo de los duplicadores. Si desea utilizar la duplicación de directorios debe crear, por ejemplo, un usuario que sea miembro del grupo de los duplicadores. El servicio de duplicación de directorios se inicia entonces con ayuda del usuario creado.

Usuarios

En Windows NT Server, los usuarios sólo disponen, en realidad, del derecho de acceso. Los derechos para modificar el sistema permanecen exclusivamente al cliente, a través del cual acceden los usuarios al servidor. Los usuarios obtienen, de manera predeterminada, el derecho de acceso a determinados directorios de Windows NT Server.

Invitados

La categoría predefinida de *Invitados* se ha creado para todos aquellos que sólo quieren acceder temporalmente a la red. Los invitados poseen derechos mínimos en el servidor y sólo pueden realizar cambios insignificantes en las estaciones de trabajo.

Todos

Todos no es en realidad ningún grupo de usuarios, al menos no aparece como tal en el Administrador de usuarios. Pero si asigna derechos de acceso en el *Explorador*, siempre se encontrará con el grupo *Todos*. Este grupo engloba a todos los usuarios que pueden acceder a los dominios. A través del grupo *Todos* se pueden asignar derechos de acceso a archivos y directorios, siempre que sean válidos para todos los usuarios del dominio NT, en lugar de hacerlo a través de usuarios individuales o grupos de usuarios.

Crear los propios grupos de usuarios

Además de los grupos predefinidos, es posible crear grupos propios con un perfil de derechos muy concreto. Para ello se puede recurrir a los perfiles predefinidos de esos grupos, o bien crear las propiedades de los nuevos grupos. También aquí se puede distinguir entre grupos locales y globales.

Vamos a crear, a continuación, un nuevo grupo de usuarios para los integrantes del departamento *Tecnología de la información.* Este grupo de usuarios está formado por administradores que entre otras tareas, deben realizar también pequeños trabajos de administración en los dominios de otros departamentos.

En primer lugar, hay que decidir si va a tratarse de un grupo local o global. En nuestro ejemplo se pretende que los integrantes del grupo de usuarios de puedan incluir en otros dominios y viceversa, que los grupos de usuarios de otros dominios de puedan incluir a su vez en este grupo para realizar allí tareas de administración. Por lo tanto, hay que crear un grupo global.

El paso siguiente consiste en darle al grupo sus usuarios. Para que el grupo de usuarios pueda trabajar también

en otros dominios de confianza (y, por lo tanto, disfrutar de determinados derechos dentro de ellos), hay que incluirlos dentro de esos dominios como grupos locales de usuarios. Todas estas configuraciones se realizan con el *Administrador de usuarios para dominios*.

Crear los propios grupos globales de usuarios

Inicie el *Administrador de usuarios de dominio.*

Seleccione la opción *Usuario, Grupo global nuevo,* defina un nombre para el nuevo grupo de usuarios y escriba una descripción del grupo.

Complete el cuadro de lista *Miembros,* seleccionando los miembros que desee para el grupo en el cuadro *No son Miembros*; a continuación, incorpórelos en el nuevo grupo de usuarios pulsando la casilla *Agregar*.

La tecla <Ctrl> le permite seleccionar varios miembros a la vez e incorporarlos juntos en el nuevo grupo.

Revise sus selecciones y confirme.

Con los pasos anteriores ha creado usted el nuevo grupo de usuarios que deseaba. El grupo aparece a partir de ahora en el *Administrador de usuarios* en el que se ha creado el grupo de usuarios, y en la lista de grupos de usuarios que se muestra en la parte inferior del *Administrador de usuarios.*

Dentro del dominio, el nuevo grupo de usuarios sólo responde a fines clasificatorios. Los integrantes de un grupo de usuarios de caracterizan normalmente por determinadas propiedades comunes a todos ellos. En nuestro ejemplo vamos a utilizar el grupo de usuarios para asignar a todos sus integrantes determinados derechos en los dominios de confianza.

Para ello hay que incorporar todo el grupo global de usuarios en un grupo local de usuarios del dominio de confianza que posean derechos específicos (por ejemplo, en le grupo local de usuarios *Administradores de impresión).*

Incorporar grupos globales de usuarios a un grupo local de un dominio de confianza.

Cree una relación de confianza entre el dominio al que haya que incorporar el grupo global de usuarios y el dominio al que pertenezca actualmente ese mismo grupo de usuarios. Para crear la relación de confianza, utilice la opción *Directivas, Relaciones de confianza* del *Administrador de usuarios* e incorpore los dominios a través del botón *Agregar.*

Active, en el *Administrador de usuarios,* las propiedades del grupo local de usuarios

en el que quiera incorporar el grupo de usuarios del otro dominio.

Pulse el botón *Agregar*. En el cuadro de diálogo *Insertar usuarios y grupos,* seleccione en primer lugar el dominio desde el cual quiere insertar los usuarios o el grupo. La lista de usuarios y grupos disponibles incluye, ahora, en sus líneas a los usuarios y los grupos globales del dominio seleccionado.

Seleccione aquí el grupo de usuarios que se acaba de crear. Incorpórelo a continuación en el grupo de usuarios del dominio actual utilizando para ello la casilla *Insertar*.

Confirme y cierre sus ajustes.

Con estos pasos ha asignado a todos los integrantes de un grupo global, determinados derechos dentro de un

dominio de confianza. Si no hubiera incluido en un grupo a todos esos usuarios, habría tenido que incorporarlos uno a uno al dominio de confianza.

Si se incorporan nuevos integrantes al dominio, a los que haya que asignar los mismos derechos, sólo tendrá que incluirlos en el grupo global de usuarios. De ese modo, obtendrán también las propiedades y derechos de todo el grupo en ese dominio. Sin los grupos de usuarios, cada nuevo usuario se tendría que dar de alta por separado en cada dominio de confianza y asignarle individualmente los correspondientes derechos.

8.4 La cuenta de usuario paso a paso

En este apartado se configurará, paso a paso, un nuevo usuario a fin de dar a conocer, los aspectos y funciones fundamentales de la Administración de usuarios de Windows NT.

Los pasos a seguir en la creación de usuarios son los siguientes:

Introducir los datos personales del usuario, en el cuadro de diálogo *Nuevos Usuarios* se especifican los datos personales del nuevo usuario. Aquí los administradores del sistema pueden tanto ejercer su poder sobre la red, como compartirlo:

− ¿Pueden elegir los usuarios sus propias contraseñas o no?

− ¿Caducan también las contraseñas(y, en caso afirmativo: es el administrador el

único que tiene derecho a revalidarlas)?.

−¿Hay que bloquear (en primer lugar) la cuenta de usuario?

Con el nombre de usuario, especificado en el primer cuadro, los usuarios pueden acceder a Windows NT Server o a cualquiera de los equipos Windows NT Workstation.

Asignarle un grupo al usuario, todos los usuarios deben formar parte de, por lo menos, un grupo. Los grupos de usuario definen los derechos que tiene cada integrante en NT Server y en la red del dominio NT.

Los grupos globales de usuarios se simbolizan con un globo, los locales con un ordenador.

Crear un perfil de usuario, al iniciar una sesión local en un ordenador de Windows NT, el nombre de usuario es el encargado, a través del perfil de usuario, de la presentación del escritorio. Al igual que sucede en las estaciones de trabajo, los clientes Windows NT 4.0 también se pueden configurar en una red Windows NT con perfiles de usuario. En el cuadro de diálogo *Perfil de entorno de usuarios*, se pueden configurar los perfiles de usuario, los *scripts* de acceso y los directorios base

Los perfiles de usuario guardan las configuraciones de pantalla del escritorio, incluida la lista inicial. Estas configuraciones de Windows NT sólo pueden utilizarse en Windows NT Workstation.

Los scripts de acceso (programas Batch), que se ejecutan en Windows NT Server cada vez que un usuario inicia una sesión en él, pueden asignar variables de entorno y vincular directorios con el ordenador de la estación de trabajo. Los scripts de registro de Windows NT Workstation se pueden ejecutar, además, en ordenadores con sistema operativo MS−DOS, Windows 3.11 y Windows 95. Juegan un papel especial en clientes Windows 3.11 y Windows 95, ya que estos sistemas operativos no son compatibles con los perfiles de usuario y las asignaciones de unidades fijas, por ejemplo, (net use..) sólo son posibles por esta vía.

Los directorios base que se asignan a cada usuario, al inicio de la sesión, son un directorio propio. Este

directorio es el primero en que se encuentra el usuario al iniciar la sesión, y con los programas Windows es, además, el directorio estándar para las opciones *Archivo, Abrir* y *Archivo, Cerrar.* El directorio base puede ser un directorio local de Windows NT Server o cualquier otra unidad de red del dominio, de libre acceso, tanto de escritura como de lectura para el usuario o su grupo.

Configurar el tiempo de acceso del usuario, cuando el servidor realiza determinadas actividades (por ejemplo la seguridad de los datos), los usuarios no pueden acceder al mismo, o bien sólo pueden hacerlo un número restringido de usuarios. Para paliar este efecto, se puede definir, para cada usuario, un horario en el que se especifique cuándo puede acceder a Windows NT Server y cuándo puede utilizar sólo determinados recursos del sistema. El rigor con que Windows NT Server mantiene estos horarios, se especifica en la configuración de seguridad. Otro motivo para la restricción temporal pueden ser determinadas normas de seguridad, por ejemplo para determinados lugares de trabajo en los que no esté permitido a nadie entrar durante el fin de semana a fin de evitar el acceso pirata.

liberar estaciones de trabajo para el usuario, cuando determinados usuarios sólo pueden acceder a NT Server desde determinadas estaciones de trabajo, estas se especifican en el botón *Iniciar desde* de las *Propiedades de usuario.* Esta restricción en los accesos de los usuarios, sólo existe para Windows NT Workstation. Otros clientes (MS−DOS, Windows 3.11, Windows 95) pueden acceder en cualquier momento.

Configurar los parámetros generales de la cuenta, en el primer cuadro de diálogo para la configuración de una cuenta de usuario, hay que definir si la contraseña de la cuenta caducará al cabo de un tiempo o no. En el cuadro de diálogo *Información de la cuenta,* se especificará si el tipo de cuenta es de duración indefinida o no.

En el mismo cuadro de diálogo se define también si la cuenta es una cuenta global o local. La opción predefinida es la cuenta global.

Con esta cuenta los usuarios del dominio de Windows NT Server o de otro dominio de confianza, pueden acceder a NT Server y ejercer los derechos otorgados a su cuenta. Las cuentas locales se utilizan para proporcionar acceso a los recursos de la red NT a usuarios de otros dominios, sin ser de confianza, e incorporarlos a grupos globales de usuarios. Estos usuarios externos no acceden directamente a Windows NT Server, sólo utilizan los recursos de la red.

Configurar, a través de la red de acceso remoto (RAS), las opciones para el acceso remoto del usuario a la red, para que los empleados de una empresa puedan acceder a la red cuando se encuentren de viaje, o desde casa, es necesario:

Dotar al equipo Windows NT Server con un módem o una tarjeta RDSI

Instalar el servicio de acceso remoto RAS

Permitir a los usuarios el acceso a través de ese servicio.

El acceso externo a la red de un empresa debe estar muy bien meditado. Incluso siguiendo todos los estándares de seguridad para redes NT, no es imposible acceder indebidamente a una red utilizando el servicio de acceso remoto RAS. A diferencia de las redes TCP/IP, las redes NT ofrecen medidas adicionales de seguridad como son los servidores *proxy* y los cortafuegos (Firewalls), para proteger a la red de empresa de la intromisión de terceros. Los servidores *proxy* y los cortafuegos hacen que el acceso a la red mediante conexión remota se realice a través de un solo ordenador. Este ordenador no sólo controla todos los accesos externos sino que los envía, también de forma restringida, a los ordenadores de la LAN.

Los datos, además, se trasmiten en texto legible a través de la línea telefónica o por tarjeta RDSI, especialmente con las conexiones *multiplex,* de modo que los técnicos ingeniosos pueden captar fácilmente la

comunicación de los empleados de la empresa. Una ayuda para impedir que así sea, la proporciona el protocolo PPTP, el cual posibilita una transmisión segura de datos a través de PPP. En el acceso remoto a su red, lo mejor que puede hacer es restringir fuertemente los derechos de acceso de los usuarios. La administración remota de NT Server se puede realizar por línea telefónica, pero pone en peligro la seguridad de todos los datos y, en consecuencia, la supervivencia de la empresa. En el cuadro de diálogo *Información de marcado* se define para cada usuario si este debe poseer acceso remoto a NT Server por línea telefónica y, en caso afirmativo, si el servidor debe responder a la llamada dado el caso.

Cuando haya introducido todos los datos que se piden en cada uno de los cuadros, ya puede incorporar el primer usuario a la lista y seguir introduciendo nuevos usuarios.

Administrar cuantas de usuario

Las configuraciones de la cuentas de usuario de pueden modificar:

Si se trata de la cuenta de un usuario, pulse dos veces el usuario en cuestión en el *Administrador de usuarios.*

Para modificar las propiedades de varias cuentas a la vez, marque todas las cuentas que se quieren modificar, mientras mantiene pulsada la tecla <Ctrl> y seleccione a continuación, la opción *usuario, Propiedades.*

Naturalmente, los nombres y las descripciones de los usuarios también se pueden modificar. Windows NT define para cada usuario un ID unívoco enlazado con el sistema de seguridad NT. Este número ID no se puede modificar bajo ningún concepto. Por eso tampoco es posible pasar un usuario de un dominio NT a otro dominio NT (porque puede ser que el ID de seguridad del usuario trasladado ya esté asignado en el nuevo dominio a otro usuario del mismo).

8.5 Definir las normas de seguridad

Windows NT soporta diferentes niveles de directivas de seguridad para la red. La seguridad de la cola de impresión y de los derechos de acceso a archivos se configuran en el *Explorador*; las normas generales de seguridad para usuarios y cuentas, así como las funciones de registro se administran, por el contrario, en el Administrador de usuarios.

Propiedades de cuenta

Cada cuenta de usuario está protegida con una contraseña (que también puede estar en blanco). Las contraseñas están para impedir el acceso de terceros al ordenador. Pero sólo cumplen esta función si:

los usuarios:

son responsables en el uso de las contraseñas y

no utilizan contraseñas demasiado fáciles de adivinar y

los administradores

controlan las contraseñas (por ejemplo, predefinido una longitud mínima para las mismas y comprobando si han sido utilizadas anteriormente por el mismo usuario)

controlando los intentos fallidos de acceso y cerrando las cuentas si es necesario, así como

persuadiendo a los usuarios para que modifiquen las contraseñas en intervalos regulares de tiempo

Las contraseñas están para proteger los recursos contra el acceso de terceros. Pero esto sólo lo consigue si se observan las siguientes reglas:

No elija contraseñas que sean demasiado cortas (que tengan un mínimo de cinco caracteres).

Las contraseñas no deben estar formadas por palabras sencillas ni contener fechas de nacimiento, nombres de amigos o de amigas ni matriculas. Todo eso resulta demasiado fácil de adivinar. Palabras como *secreto, hey*, etc... forman parte, desde hace mucho tiempo, del test estándar de los piratas informáticos.

Convenza a los usuarios de que aprendan sus contraseñas de memoria y no las apunten en ningún papel, y sobre todo, que no se les ocurra enganchar ningún papel con contraseñas en el monitor o debajo del teclado.

Para no olvidar la contraseña, es conveniente relacionarla con algo que resulte fácil de recordar.

Piense en palabras con faltas de ortografía. Cambie las mayúsculas y las minúsculas.

La unión de dos palabras a través de un carácter especial, también es un buen sistema para crear contraseñas. Cuanto menos relación guarden las palabras entre sí, tanto mejor.

Elija un verso de un poema, o un refrán, y utilice la primera letra (o la última) de cada palabra para formar la contraseña.

Modifique su contraseña periódicamente.

No utilice la misma contraseña en todos los ordenadores con que trabaja. Si alguien da con ella en uno de los ordenadores, lo hará también en los restantes.

Una parte de estas reglas se puede controlar con las opciones de seguridad para las cuentas.

Aquí están prohibidas las contraseñas demasiado cortas y se puede obligar a los usuarios a que modifiquen su contraseña en intervalos determinados de tiempo. Además, después de un número de intentos fallidos de acceso, por ejemplo 3, se puede cancelar una cuenta, o por lo menos cerrarla durante un tiempo determinado. De ese modo, se evita el peligro de los programas piratas automatizados que van probando diferentes contraseñas según determinados algoritmos (y veces también al azar).

9 REDES RAS

Aún cuando los ordenadores no estén conectados a una red local, siempre es posible conectarlos a una red a través de una línea de marcado. A este tipo de conexiones a la red, a través de líneas de marcado ("Dial−Up−Networking") Microsoft las llama RAS *(servicio de acceso remoto).* Con RAS, los ordena-dores se pueden conectar a una red con los protocolos de red TCP/IP, IPX y NetBEUI, soportados por Windows NT, y trabajar con ellos como el resto de los usuarios locales de la red.

La conexión puede establecerse tanto por línea telefónica digital como por rnódem, RDSI o cualquier otra línea apta para datos (por ejemplo, X.25).

Cuando hay conectados dos ordenadores Windows NT 4.0 directamente en-tre sí, Microsoft ofrece estrategias de seguridad específicas, por ejemplo: la posibilidad de enviar las contraseñas en clave.

En este capítulo se tratará el concepto de las redes RAS, se verá cómo debe configurarse este servicio para

módems y RDSI, y se realizarán varios viajes a través de ejemplos que mostrarán otras tantas aplicaciones prácticas concretas del servicio RAS.

9.1 El concepto de RAS

El servicio de acceso remoto le permite al cliente acceder al servidor RAS y utilizar, a continuación, todos los recursos de la red como en una LAN "nor-mal". El servicio RAS de Windows NT acepta como clientes los siguientes sistemas operativos:

Windows NT

Windows para trabajo en grupo

MS DOS a partir de la versión 3.1 (versión RAS 1. la) y

MS OS/2, versión 3.1 (versión RAS 1.1).

El servicio RAS se diferencia de los programas remotos (servicios de control remoto) de otros fabricantes. Los servicios de control remoto están pensados básicamente para la comunicación entre dos ordenadores. Estas conexiones remotas permiten realizar operaciones con archivos y ejecutar funciones de administración de sistema y, en algunos programas, también aplicaciones.

El servicio RAS, por el contrario, funciona como un encaminador multiprotocolo; a través de una línea cualquiera de datos (analógica, telefónica o digital) se establece una conexión entre el servidor RAS y el cliente RAS. Entonces se puede, en el ordenador cliente, utilizar aplicaciones y recursos del servi-cio RAS.

A continuación, se explicarán los conceptos fundamentales de las redes RAS de Windows NT 4.0. Les mostraré qué clientes pueden utilizar determinados servicios, qué protocolos se pueden utilizar en las redes RAS y cómo trabajan los servicios RAS conjuntamente con Internet. La instalación de la red RAS y la navegación a través de sus datos se tratarán en los siguientes apartados de este capítulo

Clientes de acceso remoto

Con un servidor de acceso remoto RAS, Windows NT puede establecer co-nexión con clientes RAS cuyo sistema operativo sea:

Windows NT

Windows para trabajo en grupo

MS−DOS y

LAN Manager.

Paralelamente, los servidores RAS de Windows NT ofrecen la posibilidad de utilizar los servicios RAS, a través del protocolo punto a punto (PPP), a to-dos los clientes que soporten este protocolo. Por lo general, a través de estas conexiones sólo se pueden utilizar los recursos del sistema, sin poder iniciar ninguna aplicación, ya que este protocolo no puede enviar datos de aplica-ciones.

Las conexiones RAS se pueden automatizar para que sólo se establezca co-nexión cuando realmente se necesiten datos. Si se trabaja con redes RAS Windows NT, la función AutoDial es automática; en cambio, si se trabaja con otras redes RAS de Windows, es necesario utilizar el comando rasdial. Para poder automatizar

la conexión con aplicaciones RAS de otros fabrican-tes, es necesario escribir programas especiales.

Windows NT

Las versiones 3.5 y 3.51 de los clientes Windows NT soportan todas las pro-piedades del servicio RAS. Aplican las configuraciones de seguridad del ser-vidor RAS al acceder a la red, pueden iniciar aplicaciones en el servidor RAS e interrumpen la conexión y la reinician automáticamente, cuando se producen pausas de trabajo. El protocolo PPP permite iniciar también aplicaciones TCP/IP en la red RAS.

Clientes Windows 3.1

Los clientes Windows 3.1 también soportan completamente el protocolo RAS de Windows NT. Pero no pueden establecer conexión PPP (ni PPTP) con el servidor RAS, ni enviar datos por el protocolo IPX, compatible Novell.

Windows para trabajo en grupo, MS−DOS y LAN Manager

Estos clientes utilizan la versión 3.0 del programa de acceso remoto de Microsoft. Esta versión permite utilizar todos los servicios RAS de Windows NT. Con el protocolo común NetBios se pueden utilizar en el servidor RAS, además, gateways para los protocolos IPX y TCP/IP. Los datos mismos de IPX y TCP/IP, que proporcionan los correspondientes programas del cliente RAS, no se pueden enviar.

Clientes PPP

Los servidores RAS de Windows NT funcionan también con cualquier tipo de cliente PPP que utilice TCP/IP, IPX o NetBEUI como protocolo de comunicación y envío en el nivel PPP. Estos clientes sólo pueden utilizar los ser-vicios del servidor RAS que se envíen con el mismo protocolo. Con el proto-colo de transporte se pueden enviar muy pocos servicios. Los directorios del servidor RAS, por ejemplo, no se pueden liberar con una conexión TCP/IP. En cambio, sí se pueden enviar archivos con el protocolo FTP.

Protocolos

Las redes RAS de Windows NT soportan los protocolos estándar de red: TCP/IP, NetBEUI e IPX, así como los protocolos RAS, SLIP y el protocolo RAS de Microsoft. La red RAS puede servir, por tanto, como nexo entre ordenadores de plataformas heterogéneas (Unix, Novell, PCs).

TCP/IP

Las direcciones IP sirven para identificar unívocamente cada uno de los or-denadores de una red TCP/IP.

Estas direcciones IP se pueden asignar de nuevo si es necesario, o estar configuradas de manera fija. En una red RAS de Windows NT, el servi-dor RAS puede asignar de forma dinámica direcciones IP a los clientes RAS a través del servicio DHCP (Dynamic Host Configuration Protocol).

Del mismo modo, los clientes con direcciones IP fijas también pueden acceder a la red RAS. Al hacerlo, los clientes RAS pueden utilizar direc-ciones de subred de la LAN en que se encuentra el servidor RAS. Las direcciones de subred son direcciones de redes parciales de la LAN.

Para la codificación de los clientes RAS se pueden utilizar las tablas de los servicios WINS, de los servicios DNS, así como las tablas estáticas HOST y LMHOSTS. Como estándar, los clientes RAS utilizan los servicios WINS y DNS con los mismos servidores WINS y DNS que el servidor RAS.

IPX

IPX es el protocolo estándar, hasta Netware 4.l, de las redes NetWare de Novell. Con este protocolo, capaz de encaminar, se pueden construir redes de acceso remoto (RNA).

Windows NT soporta NetWare, tanto por parte de los clientes como de los servidores. Los clientes pueden disponer de los servicios de cliente para *NetWare* y utilizar así los servicios y recursos de un servidor NetWare. El servicio de *gateway* para NetWare de los servidores NT, permite a los clien-tes NT utilizar los recursos de un servidor NetWare sin necesidad de progra-mas NetWare.

En las redes RAS, Windows NT Server puede trabajar para el cliente RAS como encaminador IPX y como *Service Advertising Protocol Agent* (agente SAP). El protocolo IPX se envía aquí casi siempre por PPP (combinación que da como resultado IPXCP, es decir, IPX *Configuration Protocol).*

Al conectarse con el servidor RAS de Windows NT, cada cliente IPX recibe una dirección IPX de red. Esta dirección la puede otorgar el servidor RAS o provenir de una dirección IPX dada por un *grupo.* El servidor RAS de Windows NT asigna las direcciones de red automáticamente con *el Router Information Protocol* (RIP) de NetWare, utilizado también por los servido-res NetWare.

Las conexiones remotas en las redes RAS no suelen establecerse a través de puras líneas de datos, sino, más frecuentemente, a través de líneas telefóni-cas, analógicas o digitales, o líneas de datos orientadas a paquetes, como X.25. Para establecer la conexión y para el transporte en esas líneas de datos, la red RAS de Windows NT necesita protocolos especiales. Aquí sólo se verá el más importante de ellos: el protocolo PPP.

El protocolo punto a punto (PPP)

Uno de los protocolos más extendidos actualmente en las conexiones a distancia para datos a través de líneas telefónicas (en serie) se llama PPP (protocolo punto a punto). Esta ampliación del protocolo SLIP (consulte más adelante), se utiliza sobre todo para conectar ordenadores con Internet a través de líneas telefónicas.

El protocolo punto a punto establece conexiones entre el servidor y el clien-te, las controla y regula el transporte básico de los datos. En una conexión establecida con el protocolo punto a punto se pueden enviar datos con cual-quiera de los protocolos de red IPX, NetBEUI y TCP/IP.

Microsoft ha ampliado el protocolo PPP con propiedades de seguridad adi-cionales. Microsoft llama a este protocolo ampliado PPTP (Point to Point Tunneling Protocol). PPTP, al igual que PPP, puede utilizarse tanto en líneas telefónicas analógicas como a través de la red digital RDSI.

9.2 Configurar RAS

El servicio RAS se puede configurar durante la instalación de Windows NT o más adelante, por separado. La instalación típica no incluye la instalación del servicio RAS.

En la instalación personalizada hay una opción que permite instalar este servicio.

Fundamentos

Para utilizar el servicio RAS se necesitan tarjetas adaptadoras para enviar los datos por líneas de conexión remota (líneas telefónicas analógicas, RDSI, X.25). Aquí supondremos que estos periféricos ya están correctamente instalados.

Información

Para instalar el servicio RAS, posteriormente a la instalación de Windows NT, es necesario estar dado de alta como miembro del grupo ADMINISTRADORES.

El servicio RAS se instala a través del icono de red del *Panel de Control de* Windows NT. Para realizar esta operación es necesario el CD de instalación de Windows NT.

Información

Cuando vaya a instalar el servicio RAS, los protocolos que vaya a utilizar con RAS ya deberían estar instalados. El servicio RAS no pregunta por estos protocolos, pero si ya están instalados, es seguro que después estarán incluidos en el servicio RAS. Si instala después, por ejemplo, el protocolo TCP/IP deberá especificarlo explícitamente en el servicio RAS.

Las siguientes instrucciones indican, paso a paso, todas las operaciones ne-cesarias para instalar el servicio RAS. La instalación es la misma para los servidores y clientes RAS en Windows NT. Cada cliente RAS puede funcio-nar también como servidor si se le permite que conteste las llamadas. Por eso al describir la instalación aquí no haremos diferencia entre servidores y clientes.

Instalar el servicio RAS

Vaya al *Panel de control* y pulse allí el icono RED.

En el cuadro de diálogo *Red,* seleccione la ficha *Servicios* y pulse el botón Agregar. Windows NT le mostrará entonces una lista de los servicios disponibles.

En el cuadro de diálogo *Seleccionar Servicio de red,* seleccione la opción *Servicio de acceso remoto.*

Ahora debe introducir la ruta de acceso de los archivos de instalación. La encontrará en el subdirectorio \I386 del CD de instalación de Windows NT.

En el paso siguiente va a configurar el puerto para el servicio RAS. En panta-lla se mostrarán todos los puertos de los modems instalados, tarjetas RDSI, tarjetas X.25 y otros puertos WAN. Si instala tarjetas más adelante, siempre puede ampliar el servicio RAS con nuevos puertos.

Windows NT intenta reconocer automáticamente los modems que todavía no estén instalados. Si no lo consigue, deberá seleccionar usted mismo el mode-lo de su módem.

Para cada puerto de una red RAS se puede definir si tiene que ser sólo de entrada, sólo de salida, o bien ofrecer ambas posibilidades.

Realice ahora las configuraciones de red del servicio RAS. Para ello, pulse el botón *Red.* En el cuadro de diálogo *Configuración de red,* confi-gure los protocolos para los servicios de cliente y servidor de su puerto RAS. Puede configurar también otros parámetros como son la codifica-ción de datos o el envío de contraseñas codificadas. Los parámetros para los servidores TCP/IP se describen en el último paso de estas instruccio-nes. Estos parámetros se pueden configurar también más adelante.

Información

Los parámetros de seguridad que introduzca aquí, sólo tienen efecto en colaboración con otros servicios RAS de Windows NI Si a su servidor acceden otros clientes RAS o si utiliza su servidor para conectar clientes RAS con otros servidores RAS, los datos y las contraseñas no se pueden codificar con RAS.

Con esto quedan finalizadas las configuraciones del servicio RAS. Salga del cuadro de diálogo *Instalación de Acceso remoto* a través del botón *Continuar* para regresar al cuadro de diálogo *Red.* Cierre este cuadro de diálogo para actualizar las configuraciones en el sistema.

A continuación debe iniciar Windows NT de nuevo para que todas las configu-raciones nuevas surtan efecto.

Ahora ya ha instalado y configurado el servicio RAS. Puede incluir nuevos modems o tarjetas RDSI siempre que lo desee. Para ello debe utilizar nueva-mente el cuadro de diálogo *Red,* ir a la ficha *Servicios* y seleccionar *Servicio de acceso remoto.* Con el botón *Propiedades* se encontrará otra vez en el cuadro de diálogo de configuración del servicio de acceso remoto., y aquí puede modificar los parámetros de los puertos instalados y agregar puertos nuevos.

Llegados a este punto, vamos a considerar más detalladamente las configu-raciones de RAS para un servidor RAS TCP/IP. En las redes TCP/IP todos los ordenadores tienen asignada una dirección IP. La dirección IP la puede traer ya el cliente RAS consigo, o recibirla asignada por el servidor.

En una red TCP/IP, las direcciones IP se pueden asignar a través del Dynamic *Host Configuration Protocol* (DHCP), o mediante las listas estáticas de di-recciones IP. Windows NT permite las dos opciones. En la primera opción, las direcciones IP se administran con el protocolo DHC. En la segunda posi-bilidad, debe indicar a Windows NT un área de posibles direcciones IP y a cada cliente RAS se le asignará exactamente una dirección IP de este área,

Utilizar un grupo de direcciones IP en el servidor RAS

Active las configuraciones de red con el icono *Red del Panel de control* de Windows NT.

En la *ficha servicios, pulse propiedades* para el servicio de acceso remoto,

Seleccione el puerto que quiere configurar con nuevos parámetros y pul-se el botón *Red.*

En el grupo de opciones *Configuración de servidor,* active el protocolo TCP/IP y, a continuación, pulse *Configurar* para definir las propiedades de este protocolo.

Active ahora la *opción Utilizar el grupo estático de direcciones y espe*-cifique las direcciones que quiere poner a disposición del cliente RAS.

Cierre los cuadros de diálogo que estén abiertos y vuelva a reiniciar el ordenador para que Windows NT active la nueva configuración en el sistema.

Los apartados anteriores han tratado del servicio RAS como tal, y de su ins-talación. Pero todavía no se ha mostrado cómo se pueden editar las propieda-des de una conexión RAS concreta. Para ello vamos a describir, en primer lugar, algunas propiedades especiales de los servidores RAS y, después, des-cribiremos cómo se establece conexión desde la red RAS con otro ordenador o con otra red.

Propiedades de un servidor RAS

Los operadores de un servidor RAS pueden permitir el acceso a otras perso-nas a los recursos del servidor, o incluso a los recursos de toda la red. Pueden decidir, por ejemplo, los protocolos con que deben acceder los clientes y determinar los protocolos necesarios para el uso de cada uno de los recursos del ordenador o de la red.

En la configuración del servicio de acceso remoto se define, entre otros, sí un ordenador puede utilizar sólo

los recursos del servidor de acceso remoto o bien los de toda la red.

Restricción de recursos

Active las configuraciones de red con el icono *Red del Panel de control* de Windows NT.

En la ficha *Servicios* pulse el botón *Propiedades* para *Servicio de acceso remoto.*

Seleccione el puerto para el que quiere configurar los nuevos valores y pulse el botón *Red.*

En el grupo de opciones *Configuraciones de servidor,* seleccione prime-ro el protocolo cuyo acceso quiere restringir o liberar y, a continuación, seleccione *Configurar*.

En el área superior de cada cuadro de diálogo de los diferentes proto-colos encontrará un grupo de opciones para regular el acceso de los clientes.

Cuando haya modificado los parámetros, cierre todos los cuadros de diálogo. Para que NT reconozca los nuevos valores deberá reiniciar el ordenador.

A un servidor de acceso remoto sólo puede acceder (y utilizar los recursos del servidor) quien posea acceso al mismo. Al igual que los usuarios de cual-quier otra red Windows NT o de un ordenador local Windows, los usuarios del servicio de acceso remoto también se administran con el *Administrador de usuarios.*

Cuando un cliente RAS establece conexión con un servidor RAS, tiene que establecerla también con el dominio, y estar registrado en el *Administrador de usuarios* para los dominios del servidor RAS.

Si el servidor RAS no está administrado por un servicio de acceso remoto de Windows NT Server, sino por Windows NT Workstation, las configuraciones a utilizar son las del *Administrador de usuarios* de Windows NT Workstation.

En la configuración previa, Windows NT no concede acceso de servicio de acceso remoto a todos los usuarios a los recursos del ordenador Windows NT o de la red. Los permisos de cada usuario hay que especificarlos indivi-dualmente en sus propiedades.

Para cada usuario se puede definir si este tiene permiso para acceder al servi-dor RAS o si el servidor RAS debe devolverle la llamada al usuario.

Cómo obtiene acceso a RAS un usuario

Abra el *Administrador de usuarios (Administrador de usuarios para do-minios* si se trata de Windows NT Server) y seleccione en dicho progra-ma los usuarios a los que quiere conceder acceso remoto al ordenador Windows NT (y tal vez también a la red).

Seleccione el botón RAS.

Configure las propiedades que desee para el usuario.

Cierre las modificaciones en *el Administrador de usuarios.*

Los usuarios de redes Windows NT están acostumbrados a ver los ordenado-res disponibles de la red en el examinador del ordenador. Lamentablemente, los ordenadores accesibles por servicio de acceso remoto no aparecen automáticamente en ese directorio. Para trabajar sin problemas con los re-cursos del servidor RAS,

este debe aparecer, sin embargo, en la lista de los ordenadores disponibles y la conexión después de seleccionar ese recurso debe establecerse del modo más automático posible.

Ambas cuestiones pueden resolverse con el servicio de acceso remoto de Windows NT. Aquí describiremos, en primer lugar, cómo mostrar un servi-dor RAS en el examinador del ordenador y, a continuación, cómo establecer una conexión automática con la función *AutoDial.* Para incorporar un servi-dor de acceso remoto al examinador del ordenador, es necesario instalar pre-viamente un adaptador de red *MS LoopBack* .

El adaptador MS LoopBack es una ayuda para convertir un ordenador aisla-do en una red sin utilizar ninguna tarjeta de red. El adaptador LoopBack simula una tarjeta de red y puede conectarse con todos los protocolos dispo-nibles de Windows NT. Así, por ejemplo, es posible compartir también en un ordenador aislado un directorio propio y conectarlo con una determinada letra de unidad. En este caso el adaptador MS LoopBack realiza la misma función que el comando *Subst* en DOS.

Incorporar servidores RAS al examinador de equipos

Pulse el icono *Red del Panel de control.*

Vaya a la ficha Identificación y configure en ella los dominios que utiliza el servidor RAS que deben aparecer en la lista de su ordenador.

Agregue ahora, en la ficha *adaptadores,* el adaptador MS *LoopBack.* Para ello necesitará el CD de instalación de Windows NT. El adaptador MS *LoopBack* utiliza un tipo muy especial de trama (frame type) para reque-rir información de otros ordenadores.

Acepte la configuración predefinida (tipo de trama: 802.3, estándar para redes Ethernet).

Vuelva a iniciar el ordenador para que cobren efecto las nuevas configuraciones de red.

El último paso consiste en conceder permiso de acceso a toda la red al servidor RAS, que debe aparecer en la lista de ordenadores disponibles. Realice esta configuración para el protocolo (activado) NetBEUI, ya que de este modo se enviarán los datos para el examinador del ordenador. Esta configuración es necesaria incluso en el caso de que el servidor RAS no posea ninguna red propia.

Una vez realizadas estas configuraciones, debe conectar su ordenador con el servidor RAS que se quiere incorporar al examinador del ordenador. Para ello deberá identificarse como miembro del dominio del servidor RAS. Cuan-do el servidor RAS quede incorporado a la lista del examinador, ya puede regresar a su propio dominio. El adaptador MS Loopback se encargará a par-tir de entonces de que el servidor RAS aparezca siempre en la lista del exa-minador del ordenador.

Después de ver estas configuraciones generales del servicio de acceso remo-to, configuraciones del servidor RAS básicamente, vamos a mostrarle en el siguiente apartado cómo establecer rápidamente, con un cliente RAS de Windows NT, una conexión con un sistema remoto y cómo se administran este tipo de conexiones. Todo ello le permitirá familiarizarse con los progra-mas de Windows NT, Conexión telefónica a la red y Monitor de marcado.

Conexión telefónica a la red

Para configurar, administrar y establecer conexiones con un servidor RAS, Windows NT utiliza el programa *Conexión telefónica a la red.* En este pro-grama se especifican los parámetros de acceso, números de teléfono y proto-colos que se vayan a utilizar para la conexión con el servidor RAS. También puede definir si se debe establecer conexión automática con el servidor RAS cada vez que se soliciten recursos de esta red remota.

En este apartado le mostraremos las propiedades más importantes de Co-nexión telefónica a la red y cómo introducir nuevas conexiones RAS en este programa. Windows NT 4.0 soporta los servicios telefónicos por ordenador, Por eso cuenta con un listín telefónico en el que guardar números de teléfono y parámetros especiales de módem para establecer conexiones por vía tele-fónica.

Todas estas configuraciones y entradas del listín telefónico se pueden utili-zar también en la red RAS para establecer conexión con un ordenador remo-to; aunque también puede utilizar la red RAS independientemente de las entradas del listín telefónico para definir sus propios parámetros de acceso, Esto último es incluso necesario cuando se utilizan modems diferentes para los servicios telefónicos y para los servicios RAS.

Iniciar Conexión telefónica a la red

El programa *Conexión telefónica a la red* se inicia desde el grupo *Accesorios* con el menú *Inicio, Programas, Accesorios, Acceso telefónico a redes.* Obtendrá entonces un cuadro de diálogo.

En este cuadro de diálogo puede seleccionar una entrada de acceso tele-fónico a redes y, a continuación, se mostrarán en pantalla los (primeros) números de teléfono correspondientes a esta entrada. Puede definir, ade-más, el lugar desde el que desee establecer la conexión.

Ahora le muestro, en un ejemplo, los pasos más importantes para configurar una conexión. Para establecer una conexión nue-va, Windows NT le ofrece un Asistente. Si ya ha configurado alguna vez una conexión telefónica a redes puede desactivar tranquilamente las explicaciones del Asistente. Eso le permitirá configurar más rápidamente la conexión.

Configurar una nueva conexión telefónica a redes

Inicie Acceso telefónico a redes y pulse el botón *Nuevo.*

El primer paso en la configuración de una conexión nueva consiste en definir un nombre para la misma.

En el segundo paso debe definir las propiedades del servidor RAS que se está utilizando. Especifique si quiere establecer conexión con Internet, si se pueden enviar contraseñas sin codificar y si el servidor RAS precisa más información sobre el acceso.

A las conexiones telefónicas a redes siempre se les asigna un adaptador en el ordenador. Seleccione en el tercer paso el adaptador que haya elegi-do. Recuerde que la selección no puede ser múltiple: no puede seleccio-nar más de un adaptador.

Introduzca ahora el número de teléfono por el que se accede al servidor RAS. Aquí puede decidir entre utilizar los parámetros de llamada del servicio telefónico de Windows NT o introducir directamente el número de teléfono con el prefijo completo.

En este, lugar todavía no se pueden indicar otros números de teléfono alternativos para el servidor RAS, los números alternativos se deben introducir más adelante en las propiedades de la conexión una vez esta-blecida.

Si en el segundo paso activó una conexión con Internet, el programa le pedirá ahora su dirección IR Si el servidor RAS le proporciona esta di-rección, no cambie la configuración predefinida de la misma: 0.0.0.0.

Para las conexiones con Internet, en el sexto paso hay que especificar, además, las direcciones de los servidores DNS y WINS. Aunque su or-denador esté conectado, además, a una red local TCP/IP, no debe utilizar las direcciones del servidor de nombres ni del servidor WINS de la red local; utilice siempre las del proveedor del servicio Internet, pues seguro que se actualizan con mayor frecuencia.

La configuración de la conexión RAS ha terminado.

Con las configuraciones realizadas ha creado una entrada de conexión tele-fónica a redes. Esta entrada aparece en la lista de los servicios de conexión telefónica a redes disponibles, de la ventana *Acceso telefónico a redes.*

Con el Asistente para crear una nueva entrada todavía no puede configurar todos los parámetros de la entrada. Utilice de momento el programa *Conexión telefónica a la red.* Seleccione en él la conexión que desee y, a continuación, el botón *Nuevo.* Ahora puede editar, a través de un sencillo menú, las propiedades de la entrada, las configuraciones de usuario y de acceso y consultar el estado de la conexión seleccionada. Este menú le permite igualmente borrar entradas de conexión telefónica a redes.

Vamos a mostrar, en primer lugar, las propiedades de la nueva conexión tele-fónica a redes. Para editarlas se utiliza la opción *Editar entrada y propieda-des del módem* del menú *Más.*

Las propiedades de una entrada del listín telefónico se editan en cinco fichas:

Básico: Lo más importante de este registro son las configuraciones básí-cas de la creación de la nueva entrada. Aquí puede seleccionar otro adaptador (para establecer la conexión a través de él) y editar los números de teléfono. En el botón *Alternativos...* puede introducir números alternativos de llamada y especificar las prioridades de los mismos en una lista.

Información

Si define varios puertos RDSI, al crear una nueva conexión telefónica a redes, Windows NT le ofrecerá exclusivamente las líneas múltiples para RDSI. Para establecer una conexión, Windows NT va probando uno a uno los diferentes puertos. En este registro puede asignarle a la nueva conexión un puerto RDSI determinado.

Servidor: La conexión telefónica a redes de Windows NT puede estable-cer conexión con otros ordenadores Windows (NT) y con servidores RAS de otras redes. En esta ficha se define el servidor RAS que se va a utilizar y el protocolo para el envío de datos por línea telefónica (SLIP o PPP). Para la conexión con un servidor TCP/IP es necesario configurar otros parámetros.

Además de las direcciones DNS, WINS y la suya propia, deberá confi-gurar otros detalles del TCP/IP. Si en la red con la que está estableciendo conexión va a ser encaminado por un encaminador predeterminado, mar-que este cuadro con una cruz.

Archivo de comandos: Algunos servidores RAS esperan que se introduzcan determinados comandos para poder ofrecer determinados servicios o entornos de usuario una vez establecida la conexión física. Estos comandos se pueden especificar en un archivo y dejar que se ejecuten automáticamente cuando se haya establecido la conexión con el servidor RAS.

Seguridad: Las redes de conexión a distancia se pueden espiar, especialmen-te si los envíos se realizan a través de las líneas telefónicas. Si no quiere perder su contraseña deberá consentir en su codificación. Lamentablemente, la contraseña codificada sólo podrá utilizarla cuando se conecte con un servi-dor RAS de Windows NT que pueda entender la codificación.

X.25: Con el protocolo X.25, orientado a paquetes de datos, las conexiones remotas con otras redes se pueden establecer también a través de líneas especiales de datos. Las propiedades de este protocolo y de la red con la que hay que establecer la conexión, se introducen en este registro. Para las conexio-nes X.25 se necesitan adaptadores o tarjetas RDSI especiales.

Las conexiones RAS asignan direcciones de red de ordenadores y recursos de una conexión RAS determinada, es decir, de un número de teléfono del listín telefónico de RAS, por ejemplo. La conexión con un servidor RAS se puede establecer automáticamente si se tiene acceso a la dirección de red de Windows NT o de una aplicación en Windows NT. La dirección de red puede ser una dirección IP, una dirección de red IPX o un nombre de ordenador NetBIOS, ya que el servicio RAS soporta cualquiera de estos tres protocolos.

Para cada conexión RAS se puede configurar la llamada automática, o no, cuando la solicite el servicio. En las conexiones automáticas también es ne-cesario confirmar la conexión con el servidor cuando se produce por primera vez. La llamada automática de una conexión se puede configurar indepen-dientemente del lugar en que se encuentre el servidor.

La petición automática o no de una conexión también se puede configurar en *Conexión telefónica a la red,* con el menú *Más.* Utilice aquí la opción *Prefe-rencias de usuario.*

Llamada automática

Active las configuraciones del usuario correspondientes a la conexión de red para la que quiere activar o desactivar la llamada automática. Para ello seleccione la conexión en la red de conexión telefónica, pulse el botón *Más* y, a continuación, la opción *Preferencias de usuario.*

En el cuadro de diálogo *Preferencias de usuario* seleccione la ficha mar-*cando.*

En la *lista activar marcado automático por ubicación,* seleccione *Nueva localización (la ubicación actual),* o sea donde la conexión debe produ-cirse por llamada automática.

Confirme y cierre los datos introducidos.

En el apartado siguiente nos ocuparemos de la seguridad en las redes de conexión telefónica y las configuraciones especiales del servicio RAS de Windows NT.

9.3 La seguridad en las redes RAS

Las redes RAS comunican ordenadores entre sí a través de líneas telefónicas y de datos. Si

es operador de un servidor RAS, está abriendo su servidor RAS, y tal vez toda la red conectada a él, al acceso exterior y si

utiliza un cliente RAS, está enviando datos importantes por líneas abier-tas al público general y deberá confiar en que esos datos no sean capta-dos por terceros de dudosas intenciones.

La seguridad en las redes RAS, por lo tanto, afecta tanto a los clientes como a los servidores RAS.

En relación con su estructura de dominios y su sistema de seguridad en gene-ral, Windows NT ofrece diferentes posibilidades a los usuarios para prote-gerse del acceso indebido de terceros. Algunas de estas medidas de seguri-dad pueden enviarse a las redes RAS. En este apartado vamos a ver:

el modo de utilizar las redes RAS dentro de un dominio Windows NT y las configuraciones de seguridad para dominios,

cómo aplicar la codificación de datos,

cómo garantizar la seguridad mediante las funciones de contestación de llamadas y

cómo controlar exactamente el uso del servicio RAS para reconocer in-mediatamente las infiltraciones en la red.

RAS en los dominios de Windows NT

El concepto de seguridad de Windows NT está basado básicamente en la agrupación por dominios de los usuarios y ordenadores con acceso a una red.

La seguridad de los dominios queda garantizada por el controlador principal de dominio y el controlador de dominio de reserva.

Para garantizar la seguridad de las redes RAS mantenidas por Windows NT Server, se pueden utilizar las configuraciones de seguridad del sistema de dominios.

Información

La seguridad en las redes RAS, no obstante, se puede garantizar también mediante otros procedimientos (por ejemplo: con redes TCP/IP o mediante el protocolo PPP) que se describirán más adelante.

Una red de conexión remota con Windows NT Server puede estar formada por un solo dominio o por varios dominios que hayan establecido entre sí relaciones de confianza. Las redes más fáciles de administrar son las que constan de un solo dominio, ya que en ese caso sólo ha y que mantener una base de datos única para todas las configuraciones de seguridad de los usua-rios y los ordenadores (base de datos de directorios).

Si trabaja con varios dominios que mantienen relaciones de confianza entre sí, puede tener problemas con los clientes RAS que utilicen la versión RAS 1. 1 de Microsoft o anteriores. Cuando un usuario accede a un servidor RAS, pero no posee ninguna cuenta en él, el servidor RAS pregunta por ese usua-rio a todos los dominios con una relación de confianza. Y después utiliza la primera respuesta para decidir si el usuario debe obtener el acceso o no. De ese modo, si el usuario posee acceso a diferentes dominios de confianza que funcionan con las mismas contraseñas y los mismos derechos de acceso, con la sola llamada del usuario no se puede saber cuál de estos dominios es el que permite el acceso y cuál, por lo tanto, es el responsable de los derechos del usuario. En ese caso, los accesos del usuario RAS deberían estar centra-lizados en el servidor RAS.

El acceso a las redes RAS que funcionan según el concepto de dominios de Windows NT, se obtiene de igual modo que en las redes locales.

Limitaciones de usuarios

En las redes RAS se pueden restringir las autorizaciones de los usuarios en las configuraciones de la base de datos de usuarios. Estas restricciones se pueden realizar a través de propiedades especiales de los protocolos o por configuraciones de red.

Los usuarios de RAS pueden quedar excluidos totalmente del acceso a los recursos de la red local en la que se encuentre el servidor RAS. Esta característica se puede configurar individualmente para cada protocolo soportado por el servidor RAS. Por ejemplo, puede conceder acceso pleno a la LAN a los usuarios RAS que accedan por NetBEUI (en el marco de su acceso de usuarios de Windows NT), y a los usuarios RAS que utilicen el protocolo TCP/IP e IPX concederles acceso solamente al servidor RAS.

El acceso de los clientes RAS a las subredes locales del servidor RAS tam-bién se puede restringir. Windows NT puede asignar uno o varios adaptadores de red a los protocolos y a determinados servicios de red. Esto es lo que se llama enlaces de los correspondientes protocolos o servicios. Restringiendo los enlaces se pueden

restringir los permisos de acceso a las redes. A conti-nuación veremos, en un ejemplo, cómo se utilizan los enlaces para restringir el acceso a RAS.

Supongamos que concede a un grupo de usuarios acceso al servidor RAS exclusivamente por el protocolo TCP/IP. El servidor RAS, que es a la vez el controlador principal de dominio de Windows NT, posee dos tarjetas de red conectadas con dos subredes físicamente distintas del dominio de Windows NT. Uno de los adaptadores de red sólo soporta el protocolo NetBEUI y el otro soporta también el protocolo TCP/IP.

Los usuarios RAS que, en este ejemplo, sólo pueden acceder con TCP/IP, sólo tendrán acceso a la subred que soporta este protocolo. Todos los recur-sos distribuidos a través de NetBEUI quedan ocultos para los clientes RAS.

Codificación de datos

Todas los envíos de datos a través de redes RAS se pueden interceptar por terceros o incluso por servicios secretos. Para que los datos importantes, pri-vados o de empresa, y sobre todo sus contraseñas de acceso a los ordenado-res remotos, queden protegidos ante semejantes accesos, se ha creado la po-sibilidad de codificar los datos para enviarlos.

Para el envío de datos codificados es necesario que el cliente y el servidor utilicen el mismo código. Este es el mayor problema que se plantea nor-malmente entre ordenadores con programas RAS de diferentes fabricantes. Incluso los productos RAS de Microsoft son diferentes para los diferentes sistemas operativos.

La codificación de datos es importante ya en el primer paso de la conexión RAS: la llamada al servidor RAS (y tal vez a toda la red). Al realizar la llamada, está enviando su permiso de acceso, es decir, su nombre de acceso y una contraseña. Si estos datos los capta alguien, existe la posibilidad de que personas ajenas a la red RAS utilicen los recursos de la red con su permiso de acceso y causen daños en su nombre.

Para evitarlo, las contraseñas sólo se envían en texto legible en los menos casos posibles. A fin de que los diferentes clientes y servidores de RAS pue-dan comunicarse con el mismo código, se han establecido directrices y pro-tocolos de ayuda.

RAS utiliza el *Challenge Handshake Authentication Protocol* (CHAP) para garantizar un envío de datos entre cliente y servidor lo más segura posible. Con este protocolo, el servidor contesta las llamadas del cliente, en primer lugar, con la codificación más segura. Si no obtiene respuesta del cliente, prueba con otras codificaciones "no tan seguras", varias veces, hasta que el cliente reaccione. El protocolo averigua, de ese modo, el nivel de seguridad con que puede enviar los datos. CHAP soporta diferentes tipos de co-dificación:

MD5, soportado por la mayoría de servidores PPP y

DES, un estándar de seguridad aceptado por el gobierno de los EE.UU. y que se utiliza por Windows NT Server desde la versión 3.5 1.

Junto al protocolo CHAP podemos mencionar otro protocolo algo menos seguro: el SPAP *(Shive Password Authentication Protocol),* utilizado por los servidores LAN de Shiva. SPAP utiliza procedimientos de codificación re-versible. Estos procedimientos proporcionan una pista sobre la codificación empleada, por lo que no resultan tan seguros como los procedimientos CHAP.

El protocolo PAP *(Password Authentication Protocol),* utilizado todavía por algunos servidores PPP, envía los datos en texto legible. Este procedimiento sólo es soportado por Windows NT RAS cuando el ordenador RAS con el que se establece la comunicación no soporta ningún tipo de codificación

Información

Con el servicio RAS de Windows NT puede desactivar las conexiones que envíen contraseñas en texto legible. De ese modo, Windows NT no establecerá conexión con el ordenador remoto si éste no soporta ningún tipo de codificación.

Además de los permisos de acceso también se pueden codificar todos los datos enviados por la red RAS Windows NT. Los estándares utilizados aquí por NT son diferentes de los utilizados para el envío de contraseñas. Las redes RAS de Windows NT codifican los datos según el RSA: Data Security Incorporated RC4−Algorithmus. Esta codificación de datos es adoptada automáticamente para cada entrada del listín telefónico y, por lo tanto, hay que desactivarla expresamente cuando el servidor RAS con el que se esta-blece conexión no soporte esta codificación.

Contestación automática de llamadas

Otro nivel de seguridad en las redes RAS es la contestación automática de llamadas. Con ella se asegura que los usuarios llamen siempre desde el mis-mo lugar. De ese modo, para que terceros puedan acceder al servidor RAS (y a la red), es necesario que consigan acceder primero al ordenador de un usuario,

La contestación automática de llamadas se configura individualmente para el usuario en las propiedades RAS. La configuración se realiza a través del *Administrador de usuarios para dominios.*

La contestación de llamadas se puede desactivar en *el administrador de usuarios,* configurarla como obligatoria o bien dejar la decisión al usuario. La contestación obligatoria es la única que ofrece una ventaja para la seguridad: sólo de ese modo se puede saber con certeza desde dónde llaman los usuarios RAS. Las contestaciones voluntarias son apropiadas para empleados que quieran utilizar los recursos de la red de empresa cuando estén de viaje; así no tienen que cargar con los costes telefónicos de ese servicio.

9.4 Redes de conexión remota seguras con PPTP

Las redes RAS pueden comunicar redes entre sí a través de líneas telefónicas o de datos. Cuando estas comunicaciones se establecen a través de Internet y del acceso RAS a los proveedores de Internet, se habla de *Virtual Private Networks (VPN).*

Las VPN representan lo contrario de las redes corporativas; en estas últimas se comunican entre sí las filiales de una empresa a través de líneas propias de datos. Pero en estas redes es necesario implantar y mantener líneas entre los diferentes nodos. Cuando estas líneas tienen que ser transcontinentales, la financiación del proyecto raramente resulta viable.

Las VPN, por el contrario, utilizan líneas que ya existen y, de ese modo, reducen considerablemente los costes de la empresa. La mayor crítica a esta solución es la falta de seguridad. Si se utilizan líneas públicas para enviar datos de una empresa:

los datos se pueden captar en su camino de A hacia B y, por lo tanto ser objeto de espionaje y

no queda excluido el acceso de terceros a la red de la empresa, ya sea por vía "pirata" o porque consigan registrar los permisos de acceso de los empleados.

Microsoft ha desarrollado un protocolo para la seguridad de las VPN. Este protocolo, el Point to Point Tunneling Protocol (PPTP), puede comunicar servidores de Windows NT entre sí, facilitando a la vez la comunicación con los proveedores de los servicios de Internet, ya que la conexión con ellos se realiza normalmente a través del protocolo punto a punto (PPP). PPTP fun-ciona también con los protocolos de

transporte TCP/IP, NetBEUI y IPX.

PPTP codifica los datos que se envían a través de PPP. Puede utilizarse tanto con otros servidores Ras de Windows NT como con los proveedores de Internet que no utilicen Windows NT. Para ello, PPTP despliega aquí los mecanismos de seguridad de CHAP (consulte más arriba) para las identifica-ciones y R4 para la codificación de datos.

Codificando los datos, con PPTP se pueden enviar también datos de los protocolos de red. IPX (Novell) y NetBEUI (Microsoft) a través de redes TCP/IP.

Para activar PPTP se utilizan las configuraciones de red para el protocolo TCP/IP. Estas configuraciones se activan desde el *Panel de control.*

Activar PPTP

Pulse el icono RED del *Panel de control.*

Seleccione el protocolo TCP/IP y abra con *Propiedades* el cuadro de diá-*logo Microsoft TCPIIP propiedades.*

Entre entonces en el registro *Dirección IP* y pulse el botón *Avanzadas.*

En las opciones avanzadas del protocolo TCP/IP, ahora ya puede activar el filtro PPTP con una casilla de opción.

Cierre sus ajustes y reinicie el ordenador para que las nuevas configuraciones cobren efecto.

En los apartados anteriores se han estudiado los fundamentos del servicio RAS y su configuración. El apartado siguiente mostrará, con ejemplos prác-ticos, cómo utilizar este servicio de manera efectiva y cómo administrar un servidor RAS.

9.5 Establecer y controlar conexiones RAS

En este apartado se verá con más detalle la utilización del servicio RAS: A través de ejemplos le mostraremos cómo establecer conexiones RAS, cómo controlar las conexiones y cómo detectar errores en el servicio RAS.

Las conexiones RAS se pueden establecer automáticamente al solicitar el servicio correspondiente. Si ha enlazado el protocolo TCP/IP con un adapta-dor de acceso telefónico a redes, la red RAS se iniciará automáticamente cuando solicite un servicio TCP/IP. Para establecer una conexión RAS ma-nualmente, inicie el programa *Conexión telefónica a la red* en el menú *Accesorios* del menú *Inicio.* A continuación, seleccione allí la conexión que de-see y establezca la conexión manualmente con el botón *Marcar.*

Información

Los términos conexión telefónica a redes y conexión RAS o red Ras, se utilizan en Windows NT, y también en este trabajo, como sinónimos.

Establecer una conexión RAS

Inicie el programa *Acceso telefónico a redes* seleccionando el mismo en el menú *Accesorios.*

En la lista de conexiones telefónicas a red configuradas seleccione la conexión que desee y pulse, a continuación, Marcar.

Indique el acceso de usuario para esta conexión.

Pulse *Aceptar*. *Acceso telefónico a redes* establece ahora una conexión. Si la conexión es por módem, se marcará el número del servidor RAS con el que quiere conectarse.

La conexión telefónica accede ahora al servidor RAS.

Cuando se establece una conexión RAS, Windows NT inicia automáticamente el programa *Monitor de marcado.* De ese modo, se pueden controlar todas las conexiones RAS, desactivar parámetros de envío de datos y cortar ma-nualmente la conexión.

Información

El programa *Monitor de marcado* se puede activar también manualmente pulsando dos veces el icono *Monitor de marcado del Panel de control* de Windows NT.

El programa *Monitor de marcado* posee las fichas *Estado, Resumen y Preferencias.*

Estado: Esta ficha contiene los parámetros actuales de envío para la lí-nea seleccionada. Con ella se puede cortar una conexión manualmente.

Resumen: Aquí puede ver una lista de todas las líneas configuradas y su uso. Se indica qué líneas son activas y cuáles inactivas.

Preferencias: En la ficha *Preferencias* puede configurar mensajes de sis-tema y la muestra en pantalla del estado al establecer conexiones RAS, así como controlar el comportamiento del *Monitor de marcado.*

En el siguiente ejemplo le mostraremos cómo el *Monitor de marcado* trae a pantalla los datos de la conexión actual.

Traer a pantalla los datos de la conexión con el *Monitor de marcado*

Inicie el programa de acceso telefónico a redes y establezca una conexión.

El Monitor de marcado se muestra en el lado derecho de la barra de ini-cio. Pulsando dos veces el icono del programa se abre su ventana.

En la *ficha estado del Monitor de marcado,* controle el envío de datos de la línea activa.

Si ahora cambia a la ficha *Resumen,* la línea por la que se está estable-ciendo la conexión RAS se muestra como línea activa.

Ahora ya puede utilizar los servicios de la red RAS. Si se ha establecido una conexión con el proveedor de Internet, también puede utilizar los servicios de Internet.

Para cortar la conexión, utilice el botón Colgar de la ficha *Estado* o de la *ficha Resumen.*

Si configura su ordenador Windows NT, no solamente como cliente RAS sino también como servidor RAS, podrá controlar las conexiones activas del servidor con el programa *Administrador de Acceso remoto.* Puede traer a pantalla una lista de los usuarios actuales y desconectar usuarios del servicio de servidor RAS.

A veces es necesario finalizar el servicio del servidor Ras o desconectar usua-rios, para liberar determinados recursos. A continuación le mostraremos en un ejemplo comentado, cómo realizar estas operaciones con el servicio de administración de RAS.

Desconectar clientes RAS

Inicie el programa *Administrador de acceso remoto* desde el menú *He-rramientas administrativas* del menú *Inicio.* En la ventana del programa podrá ver un resumen de las conexiones RAS establecidas.

Utilice la opción *Usuarios, Usuarios activos* para que se muestre en pantalla una lista de todos los usuarios activos.

Seleccione el *botón Enviar mensaje* para enviar un mensaje a todos los usua-rios que se van a desconectar de RAS.

Dé tiempo suficiente a los usuarios para que pueden cerrar la conexión por sí mismos. Si no dejan libres los recursos que están utilizando, puede desconectarlos de su servidor RAS con el botón *Desconectar*.

Confirme y cierre los ajustes realizados.

Los sucesos de la red RAS pueden seguirse con la presentación de sucesos de Windows NT. Esta presentación incluye todos los procesos de llamada y los protocolos de errores y fallos de seguridad de la red RAS.

9.6 Modificar parámetros RAS en los registros

Algunos parámetros de la red RAS sólo se pueden configurar en la base de datos de registro. Las configuraciones de la base de datos de registro hay que realizarlas siempre con precaución. Por una parte, ofrecen la posibilidad de configurar parámetros sin necesidad de cuadros de diálogo ni menús. El cua-dro de diálogo de la entrada se puede ignorar, pues los parámetros se modifi-can directamente allí donde el cuadro de diálogo correspondiente realice sus configuraciones.

Por otra parte, la base de datos de registro no sólo no muestra todos sus datos abiertamente sino que esconde, además, algunos peligros. Las configuracio-nes hechas en la base de datos de registro se incorporan al sistema sin pre-guntas de seguridad previas y, a veces, pueden paralizar todo el sistema NT. Algunas configuraciones requieren modificaciones en diferentes lugares de los registros que deben coincidir entre sí. Y esto es una fuente de error nada despreciable cuando las modificaciones se realizan directamente en la base de datos de registro.

Más adelante se describirá con más detalle la base de datos de registro. Puesto que la red RAS contiene algunos parámetros que sólo se pueden con-figurar en la base de datos de registro, esas configuraciones se tratarán aquí a continuación.

Activar archivos de registro de sucesos

Los archivos de registro de sucesos (archivos .log) sirven para registrar los sucesos de determinados componentes de un sistema operativo. Estos regis-tros se utilizan al producirse un fallo general del sistema para averiguar las causas que lo han provocado. Los archivos de registro sirven también para comprobar si alguien intenta acceder furtivamente a un ordenador.

Con la presentación de sucesos, Windows NT ofrece un archivo de registro muy cómodo. No obstante, existen algunos protocolos que no están recogi-dos en esta presentación. En el caso de las redes RAS: un protocolo PPP y un protocolo sobre el uso del controlador *(device).*

El archivo Log PPP reúne todos los sucesos PPP. Este archivo de registro se encuentra en el subdirectorio \SYSTEM32\RAS del directorio Windows NT, con el nombre de PPP.LOG. Este archivo le ayudará a localizar y resolver posibles irregularidades en las conexiones PPP.

Para activar los archivos .Log debe darle el valor 1 al parámetro Login de la base de datos de registro en:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP

En otro archivo de registro están definidas todas las comunicaciones que se producen entre los periféricos y los puertos en serie a los que están conectados, hasta que se establezca correctamente la conexión con el ordenador remoto. En las conexiones por módem se lleva un registro de todos los comandos utilizados por el módem hasta el establecimiento de la conexión. Estos registros permiten comprobar todas las variables de inicio utilizadas.

Para activar este archivo de registro, asígnele el valor 1 al parámetro Login en

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

9.7 Resumen

En este capítulo se han estudiado las redes de conexión remota que se establecen a través del servicio RAS con Windows NT. Este servicio permite establecer conexiones entre ordenadores por línea telefónica analógica, por RDSI o X.25. Las redes RAS soportan igualmente el envío de datos con i protocolos TCP/IP, NetBEUI e IPX.

Otro aspecto estudiado en este capítulo han sido las configuraciones de seguridad especiales que utiliza Windows NT en las redes RAS.

10 ADMINISTRACIÓN DE REDES

Windows NT se utiliza en las redes principalmente,

como una potente estación de trabajo tanto en redes Windows NT como en redes heterogéneas, o bien

como un servidor Windows NT que organiza y administra la red.

En este capítulo nos dedicaremos exclusivamente a Windows NT Server y describiremos la forma de administrar los servicios del servidor y de proteger los datos.

Muchos de los servicios que aquí presentaremos se pueden prestar con el Administrador de servidores: una herramienta de configuración y supervi-sión combinadas para Windows NT Server.

10.1 Administrar propiedades de los servidores

En primer lugar, nos ocuparemos de algunas de las más importantes propie-dades de los servidores, como compartir recursos, acceso de usuarios y con-trol de recursos. Ilustraremos con ejemplos la forma en que podrá controlar y manejar los recursos de los usuarios que se van a utilizar con *el Administra-dor de servidores.*

Obtener la lista de ordenadores

Inmediatamente después del inicio, el *Administrador de servidores propor*-ciona la información más sencilla que se puede ofrecer: en la ventana de la aplicación se muestra una lista de todos los ordenadores registrados en la red. De cada ordenador se indica el nombre, el tipo y la descripción de la identificación de las correspondientes configuraciones de la red.

Windows NT muestra, en esta lista, todos los servidores y clientes del domi-nio actual. También por medio del *Administrador de servidores,* se pueden administrar remotamente todos los ordenadores que operen con Windows NT Advanced Server, Windows NT Workstation o MS LAN Manager 2.x. A tal fin, se selecciona el ordenador correspondiente en la lista de ordenadores registrados y se elige la opción del menú *Equipo.* Los ordenadores que trabajen con Windows para trabajo en grupo o Windows 95 no se pueden adminis-trar remotamente por medio de esta función.

En la lista del Administrador de servidores, que contiene los ordenadores registrados, se distingue entre tres tipos de ordenadores en la red, según sus funciones:

Controladores de dominio que contienen la base de datos de seguridad de la red Windows NT y que realizan la comprobación de los usuarios que se van dando de alta.

Windows NT Server que se utiliza en la red como servidor de aplicacio-nes, de archivos o de tareas de impresión, pero que no puede aceptar altas de usuarios.

Todos los restantes ordenadores de la red.

Cuando sólo desee mostrar en esta lista un determinado tipo de ordenador, lo podrá realizar con el menú Ver. La tecla F5 o la opción del menú Ver, Actua-lizar, pueden actualizar la lista de los ordenadores registrados.

Con el Administrador de servidores también se pueden administrar servido-res y estaciones de trabajo de otros dominios. Como es lógico, en estos do-minios se tiene que crear una relación de confianza y tiene que existir un acceso como operador de cuentas o administrador. En caso contrario se mos-traría, como sucede al abrir la lista del administrador de servidores en el dominio propio, la lista de los ordenadores registrados, pero no se podría modificar ninguna de las configuraciones.

Información

Si el dominio que pretende administrar con el Administrador de servidores se encontrase en una red de área extensa, estructurado mediante conexiones lentas (por ejemplo, módems), el ordenador ofrecerá unos tiempos de respuesta muy largos a las preguntas del Administrador de servidores. Para que este hecho no sea interpretado como un error, podrá informar previamente al Administrador de servidores sobre la lentitud de las conexiones mediante Opciones, Conexión a baja velocidad.

Solicitar propiedades de servidores

Podrá solicitar, y también administrar, las propiedades de cada servidor in-cluido en la lista de ordenadores registrados, y que se haya configurado para administrar local o remotamente. Pero, en cualquier caso, para poder modifi-car las configuraciones de las propiedades del servidor, tendrá que estar autorizado para acceder como operador de cuentas o como administrador del servidor.

Las propiedades de los servidores se obtienen:

seleccionando el servidor en la lista y eligiendo el menú Equipo, Propie*dades*

seleccionando el servidor en la lista y pulsando *Aceptar,* o bien

pulsando dos veces el servidor de la lista.

Información

En todos los casos se mostrará el cuadro de diálogo con las propiedades del servidor. Si abre este cuadro de diálogo mediante el icono *Servidor del Panel de control,* se mostraran únicamente los servidores locales. La selección efectuada por medio del *Administrador de servidores l*e también este servicio para los restantes servidores de la red dotados de la función de administración remota.

En primer lugar, el cuadro de diálogo *Propiedades de...* proporciona dentro del área *Resumen* unos sencillos datos estadísticos sobre el grado de utilización del servidor:

Sesiones: El número total de usuarios que han iniciado sesión en este servidor.

Archivos abiertos: La cantidad de recursos utilizados en el servidor selec-cionado.

Bloqueos de archivos: La cantidad de bloqueos de archivos en este servi-dor que, como consecuencia, ha ocasionado el agotamiento del número máximo de accesos compartidos permitidos.

Canalizaciones abiertas (NAMED PIPES): La cantidad de canalizacio-nes abiertas. Estas son comunicaciones especiales que se establecen en-tre los distintos procesos de un ordenador y los de otro conectado a él,

Con los botones situados en el borde inferior del cuadro de diálogo *Propiedades de...* podrá obtener más información del servidor y efectuar configu-raciones; describiré éstas en los apartados siguientes.

Sesiones de usuarios

A los administradores de sistema les interesa conocer las informaciones so-bre el grado de utilización de la red en todo momento. Éstas sirven de ayuda para dictaminar la capacidad de los servidores y para decidir las cuestiones relacionadas con sus ampliaciones.

Estas informaciones se obtienen del *Administrador de servidores con Pro-piedades de...* del servidor y el botón *Usuarios.*

En la lista de usuarios conectados se muestran y especifican todos los usua-rios conectados con el servidor,

el tipo de ordenador que utilizan estos usuarios

el tiempo que llevan conectados

sus periodos de inactividad y

si se han conectado en calidad de invitados.

Los recursos utilizados por un usuario determinado se muestran en un se-gundo cuadro de listas situado debajo de la lista de usuarios. Para ello, tendrá que seleccionar previamente un usuario en el cuadro de lista superior. En la lista se mostrarán los recursos utilizados en

directorios y archivos compartidos

canalizaciones

impresoras compartidas

colas de espera para acceso telefónico a redes (sólo MS LAN−Manager 2.x) y

recursos no reconocidos.

Por medio de la verificación de los recursos abiertos y de los períodos de inactividad, los administradores de sistema supervisan los recursos que se están utilizando innecesariamente:

Para determinados programas, en las redes, sólo existe un número reducido de licencias para ordenador por razones económicas. A título de ejemplo, en su red no necesitará una licencia del programa de gestión de costes para cada uno de los ordenadores, si son sólo tres las personas que utilizan ese progra-ma. De otras aplicaciones tendrá también suficiente con un número de licen-cias inferior al número máximo de posibles usuarios, ya que, en condiciones normales, no todos suelen trabajar simultáneamente con el mismo programa.

Como es lógico, este procedimiento funciona cuando no todos los colabora-dores inician por las mañanas el ordenador y todas las aplicaciones con las que posiblemente empezarán a trabajar más tarde. Con objeto de liberar re-cursos para otros usuarios, se tienen que cerrar todas las aplicaciones nada más concluir el trabajo con ellas.

En las sesiones de usuario, los administradores de sistema comprueban quién, cuándo y qué recursos se han abierto y cuánto tiempo han estado ociosos. De esta forma aparecen "cadáveres informáticos", como consecuencia de caídas del sistema o programas que no devuelven adecuadamente sus recursos des-pués de ser cancelados por el usuario.

Como miembro del grupo de administradores y haciendo uso del *Adminis-trador de servidores* podrá desconectar a un usuario todos los recursos que utilice o sólo los seleccionados.

En el apartado siguiente mostraremos la forma de desconectar a un usuario para que no pueda operar en la red. En otro apartado posterior describiremos la forma de desconectar los recursos seleccionados.

Información

Sin más explicaciones, Windows NT puede desconectar a los usuarios todos lo recursos que hayan utilizado en su sesión. Conscientes de la plena responsabilidad de su "poder", los administradores de sistema deberían evitar estas situaciones. Si a un usuario que está trabajando con Word se le retirase involuntariamente este recurso, perdería irrecuperablemente todos los archivos que no hubiera guardado.

Desconectar usuarios

Inicie *el Administrador de servidores,* seleccione el servidor en cuestión en la lista de los ordenadores registrados del dominio y obtenga las pro-piedades de este servidor.

En el cuadro de diálogo *Propiedades de...* pulse el botón *Usuarios.*

En el cuadro de diálogo *Sesiones de usuarios en....* seleccione el usuario que desea desconectar.

Pulse el botón *Desconectar* para concluir la sesión del usuario. Al usua-rio se le retiran inmediatamente, y sin ninguna explicación, todos los recursos utilizados en la sesión activa.

Controlar los recursos compartidos

Con el *Administrador de servidores* podrá también controlar, y en su caso bloquear, los recursos compartidos de cada servidor administrado local o remotamente en el dominio seleccionado. En el cuadro de diálogo *Propieda-des de....* seleccione el botón *Compartidos* y seleccione el nombre del recur-so que aparece en el cuadro de diálogo *Recursos compartidos en....*

También en esta lista Windows NT distingue los diferentes recursos por me-dio de iconos. Con los botones *Desconectar y Desco-nectar todos* podrá desconectar un recurso a los usuarios seleccionados o a todos. Windows NT retira la conexión sin previo aviso. Debería informar previamente al usuario o usuarios de este hecho.

Con el *Administrador de servidores* podrá editar directamente las propieda-des de un recurso compartido y asignar nuevos recursos como compartidos.

Con Recursos compartidos en... del Administrador de servidores no podrá modificar las condiciones de seguridad de los recursos compartidos (ampliación de autorizaciones, supervisión, posesión...). Sólo podrá modificar es-tas propiedades desde el botón *Compartir* de las propiedades de una unidad o directorio. Estas son:

el propio recurso compartido (por ejemplo: la aplicación)

el nombre del recurso compartido

la cantidad de usuarios admitidos y

las autorizaciones pertinentes para los usuarios y grupos de usuarios del dominio.

Para editar un recurso compartido de un servidor o de una estación de trabajo remota, seleccione el ordenador en la lista de servidores y estaciones de tra-bajo y seleccione el menú *Equipo, Recursos compartidos.* En el cuadro de *diálogo Directorio compartido podrá:*

obtener una lista de los recursos compartidos en el ordenador

instalar nuevos recursos compartidos

editar propiedades de recursos compartidos y

desconectar los recursos compartidos.

Información

La creación de nuevos recursos compartidos con el *Administrador de servidores es,* por desgracia, de complicado manejo. Tendrá que escribir, en un cuadro de texto, la ruta de acceso del recurso a compartir. No se podrá explorar, a continuación, la red ni la lista de los ordenadores locales. Para ello instale, de forma centralizada, los recursos compartidos de los ordenadores administrados remotamente en la red.

Generalmente se suele utilizar el *Administrador de servidores* para editar las propiedades de los recursos compartidos de los ordenadores de la red. Así, por ejemplo, podrá aumentar el número permitido de usuarios de un recurso en cualquier ordenador remoto de la red, cuando se produzcan cuellos de botella y queden aún licencias disponibles.

En el apartado siguiente mostraremos cómo funciona esto.

Aumentar el número de usuarios de un recurso

Inicie el *Administrador de servidores* y seleccione el ordenador cuyos recursos desea editar.

Elija el menú *Equipo, Recursos compartidos.*

En el cuadro de diálogo *Directorio compartido* seleccione, en el cuadro de lista *Directorios compartidos en...* el directorio cuyas propiedades desea editar y pulse el botón *Propiedades.*

Modifique el número permitido de usuarios del recurso.

Confirme sus cambios.

Recursos utilizados

En los apartados anteriores hemos visto cómo se controlan y manejan los recursos con el *Administrador de servidores* de una forma totalmente gene-ralizada. De esta forma, sólo podía conocer el número de usuarios que utili-zaban un determinado recurso en un momento dado, o el número de usuarios conectados al servidor seleccionado. A veces es interesante conocer además los archivos que utilizan los usuarios. El *Administrador de servidores tam*-bién nos servirá de ayuda en estos casos.

En las propiedades de un ordenador de red, se puede obtener por medio del botón *En uso* una lista detallada de todos los recursos abiertos.

El cuadro de diálogo *Recursos abiertos en...* proporciona un resumen esquematizado acerca de

los usuarios

el acceso y

los bloqueos de un archivo.

Alertas y mensajes

En los apartados anteriores le hemos mostrado algunos procedimientos de trabajo de los *Administradores de sistema* que desconectan a los restantes usuarios de la red, de todos los recursos o algunos de ellos. En este apartado le mostraremos la manera de informar a los usuarios con el *Administrador de servidores* y el servicio de mensajes de Windows NT sobre las acciones pre-cedentes.

Al producirse algunos sucesos (por ejemplo: la desconexión del sistema), Windows NT envía automáticamente mensajes que alertan a los usuarios de tal suceso. Poco comprensible es el hecho de que no se envíen automática-mente también tales informaciones cuando se produce alguna intervención en los recursos compartidos o en los recursos abiertos, ya que ello podría provocar una pérdida de datos del usuario.

En primer lugar, describiremos en un apartado cómo y a quién podrá enviar alertas como administrador de la red.

Activar mensajes de alerta

Inicie el *Administrador de servidores* y obtenga las propiedades del or-denador cuya lista de distribución para mensajes de alerta desee editar.

Pulse el botón *Alertas* del cuadro de diálogo *Propiedades de....*

Incluya en la lista todos los ordenadores que tienen que recibir las alertas de este ordenador. Desgraciadamente no podrá seleccionar los nombres de ordenadores en una lista, sino que tendrá que escribirlos.

Cierre los cuadros de diálogo. Para que las asignaciones efectuadas pue-dan entrar en vigor, tendrá que iniciar de nuevo el ordenador. Por lo tan-to, tendrá que abandonar su cómodo sillón de administrador e ir a visitar personalmente a los correspondientes ordenadores de la red.

Para que se puedan enviar las alertas, tendrán que estar instalados e inicia-dos el *servicio de alerta* y el *servicio de mensajería.* En Windows NT Server estos servicios están incluidos en la instalación estándar e iniciados de forma estándar también por el servidor. Con el *Administrador de servidores podrá* comprobar si el ordenador en el que está trabajando tiene instalados tales servicios.

Seleccione, en el *Administrador de servidores,* el ordenador en cuestión, y elija el menú *Equipo, Servicios,* para abrir el cuadro de diálogo *Servicios en...* En los ordenadores locales accederá a este cuadro de diálogo mediante el icono *Servicios del Panel de control* de Windows NT.

Los ordenadores que tienen que recibir los mensajes, tienen que tener inicia-do el servicio de mensajería. Sólo los ordenadores en Windows NT, OS/2, Windows 95 y Windows para trabajo en grupo, pueden recibir directamente estas informaciones, ya que poseen servicios de mensajería compatibles. Las estaciones clientes en MS−DOS, sólo soportan la versión 3.0 del servicio de mensajería del cliente NT. En cualquier caso, la recepción de mensajes se tiene que activar por separado.

Información

Los productos de Microsoft Windows para trabajo en grupo y Windows 95 utilizan para ello el programa WINPOPUREXE, que se encuentra en el directorio raíz Windows. Como administrador de sistema, debería agregar obligatoriamente este programa en el archivo Autoexec.bat de la estación cliente (o iniciarlo automáticamente mediante un archivo de comandos) para activar el servicio de mensajería en este ordenador.

Los ordenadores Windows NT utilizan un servicio de mensajería propio, que muestra las informaciones en una ventana pequeña. Las informaciones pro-pias se pueden enviar desde *el administrador de servidores* o desde *la interfaz de comandos* (consulte más adelante).

Uno de los mensajes de advertencia más importantes es la desconexión de un servidor. Para comprobar que el envío de mensajes sigue funcionando duran-te la desconexión, tendrá que desconectar el ordenador dos veces: una vez para guardar las asignaciones recién efectuadas; en este caso, tendrá que in-formar a los usuarios de esta acción; la segunda vez porque, a continuación, hay que enviar un mensaje a todos los usuarios.

Ya hemos experimentado que el propio Windows NT es algo tranquilo a la hora de enviar mensajes. Hace falta por ello que, en caso de configuraciones de sistema urgentes, envíe los mensajes.

Incluso antes de la desconexión de un ordenador, podrá enviar adicionalmente un mensaje propio para que los usuarios dispongan de más tiempo para po-der realizar las copias de seguridad de sus datos y para la desconexión del propio ordenador.

Le presentamos, en este momento, dos tipos de mensajes diferentes en los apartados siguientes:

Mensajes a todos los usuarios que estén conectados a un determinado ordenador de la red.

Mensajes a un determinado ordenador completo.

Enviar mensajes a todos los usuarios

Inicie el *Administrador de servidores* y seleccione el ordenador al que tie-ne que enviar los mensajes.

Elija el menú *Equipo, Enviar mensaje.*

Introduzca el mensaje en cuestión.

Confirme su mensaje con *Aceptar* para enviarlo a todos los usuarios.

Recuerde que sólo los ordenadores con el− servicio de mensajes activado pue-den recibir ese mensaje.

A veces ocurre que el mensaje no atañe a todos los usuarios. En este caso, envíe el mensaje sólo a los ordenadores correspondientes para no crear inne-cesariamente confusión entre los usuarios.

net send Nombre_de_ordenador Mensaje

Enviar mensajes a algunos usuarios

Inicie una solicitud de entrada.

Para enviar el mensaje: "Atención: se retiran recursos" al ordenador"486", escriba el comando:

net send 486 Atención, se retiran recursos

En general, el formato del comando es:

net send Nombre_de_ordenador Mensaje

Windows NT representa los mensajes en un cuadro de diálogo pequeño.

10.2 Administrar miembros del dominio

El *Administrador de servidores* se puede utilizar también para administrar algunas configuraciones de seguridad de los dominios de Windows NT. Mos-tramos aquí cómo se puede utilizar el administrador de servidores en la ad-ministración de dominios.

Definición del controlador de dominio

El elemento esencial de la concepción de seguridad de una red Windows NT es el controlador de dominio. Este es un servidor Windows NT que contiene la base de datos de seguridad (Directory DataBase) con todos los datos de los usuarios y las informaciones sobre recursos y permisos de acceso a la red.

Todo dominio necesita un controlador principal de dominios (PDC) que con-tenga y administre esta base de datos. A veces, y a efectos de simplificación, se suele denominar a este controlador "controlador de dominio". Sólo duran-te la instalación de Windows NT, podrá instalar un controlador principal de dominio para un nuevo dominio de Windows NT. Si instala el primer servi-dor de un nuevo dominio simplemente como servidor, este carecerá de funcionalidad de red.

Si su dominio contiene un controlador principal de dominios, todos los ser-vidores Windows NT restantes

funcionarán como controladores secundarios de dominios (denominados también controladores de seguridad de dominios de seguridad o de copias de seguridad). El controlador principal de dominios copia su base de datos de usuarios en este servidor y cada 5 minutos actuali-za su contenido con el de los otros servidores.

Los controladores principales de dominio pueden tener fallos durante largo tiempo y quizá, alguna vez, exija unos trabajos minuciosos de mantenimien-to. Sin embargo, ninguna red Windows NT trabaja sin un controlador princi-pal de dominio. Si carece de controlador de dominio de reserva, tendría que suspender el trabajo en red. Si su red dispone de al menos un controlador de dominio de reserva (es decir, otro Windows NT Server cualquiera), podrá ascender a este a controlador principal de dominio. Contendrá ya una copia de la base de datos de usuarios, actualizada por el controlador principal de dominio. Descienda al controlador principal de dominio a servidor y apá-guelo para que entren en vigor las modificaciones necesarias.

Podrá efectuar los ascensos y descensos de controladores de dominio con el *Administrador de servidores* de Windows NT. Como es natural, es requisito imprescindible que cuente con otro servidor en la red, que pueda convertirse en controlador de dominio de reserva.

Cambio del controlador principal de dominios

Inicie el *Administrador de servidores* y seleccione el ordenador que se va a promover a controlador principal de dominio.

Elija el comando *Equipo, Promover a controlador principal de dominio.*

El anterior controlador principal de dominio recibe automáticamente el *sta-tus* de servidor siempre que continúe registrado en la red. Esto es absoluta-mente necesario porque las redes Windows NT no permiten la conexión de usuarios y ordenadores cuando se encuentren activos dos controladores prin-cipales de dominio.

Sugerencia

Si estuviera fallando el anterior controlador principal de dominio, tendrá que descenderlo con *el administrador de servidores* para que la red pueda seguir operativo. A tal fin seleccione el controlador de dominios y elija, a continuación, la opción del menú *Equipo* para convertir el controlador principal de dominio en controlador de dominio de reserva.

Procediendo de igual forma, podrá poner de nuevo en servicio, tras el fallo, el anterior controlador principal de dominio.

Sincronización de la base de datos de seguridad

El controlador principal de dominio coteja periódicamente su base de datos con las de todos los demás servidores de la red de Windows NT. Podrá forzar manualmente la ejecución de esta sincronización con *el Administrador de servidores* cuando, por ejemplo, la base de datos de seguridad de un servidor haya dejado de ser actual.

El *Administrador de servidores* distingue entre dos tipos de sincronización: uno, la sincronización de la base de datos de seguridad del controlador prin-cipal de dominio con la de otro único ordenador; y otro, la sincronización de la base de datos de seguridad con las de los restantes servidores de la red.

En el primer caso, seleccione el servidor cuya base de datos se tenga que sincronizar con la del controlador principal de dominio, y elija la opción *Equipo, Sincronización con el controlador de dominios* .

Si se tienen que sincronizar todos los servidores, seleccione el controla-dor principal de dominio con el administrador de servidores y elija la *opción Sincronizar el dominio completo* del menú *Equipo.*

Antes de efectuar la sincronización de todo el dominio, el *Administrador de servidores* advertirá que este proceso puede durar algunos minutos. Dado que durante todo ese tiempo, la red estará muy cargada, su funcionamiento normal se verá limitado. Durante ese tiempo, además, no se podrá conectar ningún nuevo usuario al dominio de Windows NT.

Incluir ordenadores en un dominio

Para que un ordenador pueda sacar provecho de los recursos de un dominio de Windows NT, tiene que estar incluido en ese dominio. A todo ordenador incluido en un dominio, se le asigna una entrada (una cuenta de ordenador) en la base de datos de seguridad del controlador de dominios de Windows NT.

Existen varias formas de incluir un ordenador Windows NT en un dominio:

Al instalar el ordenador podrá determinar, en las configuraciones de la red, si el ordenador se tiene que registrar en un dominio de Windows NT y cuál va a ser su nombre. Si el usuario del ordenador posee derecho de acceso al dominio, el ordenador se incluirá en el dominio al conectarse por primera vez y se creará la cuenta de ordenador para él.

Tras la instalación, y como miembro del grupo *Administradores o* Admi-*nistradores de dominios*, podrá incluir posteriormente el ordenador en un dominio. A tal fin, seleccione en el *Panel de control* el icono *Red* y, a continuación, la ficha *Identificación.* Con el botón *Cambiar* podrá in-cluir el ordenador en otro dominio y solicitar la asignación de una cuenta de ordenador en ese dominio. No obstante, necesitará para ello el nom-bre con que se haya registrado y la contraseña de un miembro de alguno de los grupos *Administradores, Administradores de dominios u Opera-dores de cuentas* del dominio en cuestión.

Con el *Administrador de servidores* podrá incluir en un dominio cual-quier ordenador que esté físicamente conectado a la red actual. A tal efec-to, utilice la opción *Equipo, Agregar al dominio.*

Al incluir un nuevo ordenador en un dominio, podrá distinguir entre un orde-nador que actúe como estación de trabajo (o un servidor que no haya recibi-do ninguna copia de la base de datos de seguridad) y un controlador de domi-nio de reserva.

Advertencia

¡Al ejecutar este procedimiento creará un vacío de seguridad por un breve periodo de tiempo! Cuando incluya un nuevo ordenador como controlador de dominio de reserva, el ordenador recibirá, al realizar el primer inicio, una copia de la base de datos de seguridad del servidor. Si otro ordenador de la red utilizara el breve intervalo de tiempo transcurrido entre la instalación del nuevo ordenador en el dominio con el *Administrador de servidores* y el propio registro de este ordenador en el dominio, se podría registrar con este nombre de ordenador como controlador de dominio de reserva y conseguir acceder sin autorización a la base de datos de seguridad. Por todo ello, el nombre del nuevo ordenador se debería adjudicar precisamente cuando el ordenador se haya registrado ya por primera vez en él dominio de Windows NT y, por lo tanto, cuando ya contenga una copia de la base de datos de seguridad.

10.3 Duplicación de directorios

Con la duplicación de directorios podrá enviar el contenido de los directorios de un Windows NT Server de una red a otro Windows NT Server o Workstation de la misma red. Los directorios del ordenador están permanentemente comunicados entre sí, de tal forma que los usuarios puedan acceder al azar y siempre

obtengan la misma información.

La duplicación de directorios se realizará siempre entre dos ordenadores de una red Windows NT y no se podrá regular por ninguno de los distintos usua-rios de ese ordenador.

Información

Windows NT duplica siempre los directorios en una sola dirección (unidireccional): existen servidores de exportación y servidores de importación que reproducen los datos del servidor de exportación. Como servidores de exportación sólo se pueden utilizar ordenadores Windows NT, ya que sólo ellos cuentan con el servicio de reproducción de directorios. Los ordenadores Windows NT Server, Workstation y OS/2−LAN−Manager pueden hacer las veces de servidor de importación. Los directorios y archivos exportados tienen que satisfacer los acuerdos sobre nombres existentes en el sistema de archivos vigente en el otro ordenador.

La exportación de datos no tendrá que hacer referencia necesariamente a un ordenador determinado, también se podrá realizar esa exportación hacia un dominio de Windows NT en general. Puede importar esos datos todo ordena-dor Windows NT u OS/2 que esté registrado en ese dominio.

Del mismo modo, como ordenador de importación se puede asignar la importación de cierto directorio de un ordenador determinado o importar, en general, los datos de todo un dominio.

Un archivo del servidor de exportación se duplica cuando se crea por prime-ra vez en el directorio de exportación y, a continuación, con cada modifica-ción del archivo.

El servicio de duplicación de directorios se puede utilizar para distribuir por la red accesos de lectura a determinados datos. Es decir, podrá sugerir a al-gunas de las estaciones clientes de la red que no accedan a la propia fuente de datos, sino a la duplicación existente en algún servidor de la red. Sin embargo, dado que la exportación de directorios es unilateral, es decir, sólo se actualiza por el servidor de exportación, sería conveniente no utilizar este procedimiento con los directorios sobre los que los clientes tengan acceso de escritura.

Todo servidor de exportación usa, como ruta de acceso predeterminada, el *subdirectorio \System32\Repl\Export*, que se encuentra en el directorio raíz de Windows NT. Todos los archivos y subdirectorios de este directorio se envían al directorio *\System32\Repl\Import* del servidor de importación. Por desgracia, los datos de otras estructuras de directorios no se pueden exportar con el servicio de duplicación.

Los datos del servidor de exportación se pueden encaminar inmediatamente hacia todo servidor de importación. Dado que con ello se envían a veces directorios parcialmente actualizados, sólo se podrán enviar estos datos cuan-do el contenido de ese directorio no vaya a experimentar modificaciones en un intervalo de unos dos minutos al menos.

Algunos directorios del servidor de exportación se pueden bloquear para la exportación en cualquier momento y los datos de los servidores de importa-ción se pueden "congelar" en un estado determinado.

En los apartados siguientes le mostraremos cómo se instala y utiliza el servi-cio de duplicación de directorios.

Instalar la duplicación de directorios

El servicio de duplicación de directorios tiene que haberse instalado previa-mente durante la instalación inicial, como cualquier otro servicio de los or-denadores Windows NT. En la instalación predeterminada de

Windows NT sucede así. El servicio tiene que estar activo en el servidor de exportación y, sobre todo, en los servidores de importación. Podrá verificar este hecho en cada ordenador mediante el icono *Servicios del Panel de control* o consul-tando los servicios con el administrador de servidores y buscando, a conti-nuación, el *Servicio de duplicación.*

Sin embargo, antes de que se pueda hacer uso de este servicio, se tiene que agregar una cuenta de usuario para la duplicación de directorios; tiene que tratarse de un miembro del grupo de operadores de seguridad. Con esta cuen-ta de usuario se registran todos los servidores de importación en el servidor de exportación; el servidor de exportación envía los datos. Para que el servi-cio de duplicación pueda utilizar la cuenta de usuario,

la contraseña de la cuenta no debe caducar nunca

se tiene que poder registrar en la cuenta las 24 horas del día (sin periodos de exclusión) y

el usuario de la cuenta tiene que ser miembro del grupo de operadores de seguridad.

La instalación de cuentas de usuario se ha descrito ya anteriormente. No utilice el nombre *Duplicador* para la cuenta de usuario, porque ya existe un grupo de usuarios con el mismo nombre en Windows NT. La cuenta de usuario para el servicio de duplicación tiene que ser válida en todos los servido-res de exportación e importación de la red.

Una vez en nuestro poder la cuenta de usuario, se podrá instalar el servicio de duplicación. A tal fin se edita este servicio con el cuadro de diálogo *Servicios,* al que se llega mediante el *Panel de control* o a través de la red con el *Administrador de servidores* y el menú *Equipo, Servicios.*

Seleccione el *Duplicador de directorios* y, a continuación, pulse el botón *Inicializar.*

Seleccione el tipo de inicio automático. En este caso el servicio de duplica-ción se tiene que registrar automáticamente con la cuenta recién instalada.

Por lo tanto, seleccione, en el grupo *Iniciar sesión como,* la opción *Esta cuenta* e introduzca, a continuación, la cuenta del servicio de duplicación. Podrá seleccionar esta cuenta en la lista de todas las cuentas disponibles pulsando el botón situado a la derecha del cuadro.

A continuación, el sistema le confirmará que la vinculación de su cuenta con el servicio de duplicación de directorios se ha efectuado satisfactoriamente.

En el paso siguiente ya podemos instalar el servidor de exportación, es decir, determinar los directorios que se vayan a duplicar y de qué forma se hará.

Configuración del servidor de exportación

Después de que el servicio de duplicación se haya instalado como tal, ya podemos configurar el servidor de exportación. Se tienen que instalar las funciones del servidor de exportación siguientes:

Selección de los directorios originales que se tengan que copiar en el servidor de importación para su duplicación.

Creación de una lista de ordenadores o dominios autorizados para la im-portación de datos.

Exportación de los datos a unos ordenadores determinados o exportación a todos los dominios.

Para instalar el servidor de exportación no es necesario que existan todos los datos y subdirectorios. Windows NT instala el directorio predeterminado al instalar el servicio de duplicación.

Para instalar el servicio de duplicación utilice el cuadro de diálogo *Servidor* al que puede acceder localmente por medio del *Panel de control* o a través de la red con el *Administrador de servidores.* Pulse el botón *Duplicación del* cuadro de diálogo *Servidor* (si ha accedido localmente) o en el de *Propieda-des de...* (si ha accedido a través del Administrador de servidores).

Seleccione la opción *Exportar directorios* y seleccione la ruta de acceso de los datos que se vayan a exportar. Si estos datos se encontrasen en el directo-rio principal de la ruta de acceso predeterminada, no haría falta realizar nin-guna otra acción.

En caso contrario, pulse el botón *Administrar* e incluya los subdirectorios del directorio de exportación.

En este cuadro de diálogo podrá establecer también si los datos se tienen que duplicar inmediatamente con modificación, o si el servidor de exportación tiene que esperar a que se hayan estabilizado los directorios. En este último caso, el servidor de exportación da lugar a una espera predeterminada de dos minutos. Pulse la casilla de verificación *Subárbol completo* para incluir tam-bién los subdirectorios del directorio actual en la exportación.

Con este cuadro de diálogo podrá bloquear algunos directorios de expor-tación.

En el siguiente paso especifique qué ordenadores o dominios estarán autorizados para importar datos. Agrégelos a la lista de los servidores de exportación con el botón *Agregar* del cuadro de diálogo *Duplicación de directorios* y seleccionando en la lista de ordenadores y dominios disponibles, los ordenadores o dominios adecuados.

Cierre todos los cuadros de diálogo. El servidor de exportación ya está configurado para la duplicación de directorios.

Configuración del servidor de importación

Como servidor de importación se puede elegir tanto Windows NT Server como Workstation. La instalación del servidor de importación se realiza de igual forma que la del servidor de exportación. Seguramente reconocerá al-gunas configuraciones de los cuadros de diálogo, ya que se presentaron en el último apartado.

Edite de nuevo las propiedades del servidor, obteniéndolas por medio del *Panel de control* o del *Administrador de servidores.* Con el botón *Duplica*-ción accederá otra vez al cuadro de diálogo *Duplicación de directorios, y* edite en la parte derecha del cuadro de diálogo las propiedades del servidor de importación. De la misma forma como se procedió con el servidor de exportación, indique los directorios que se van a duplicar y los servidores o dominios que tengan que tener dispuestos esos datos. También en este caso se pueden bloquear algunos directorios y excluirlos temporalmente de la duplicación.

Errores en la duplicación de directorios

Los errores del servicio de duplicación de directorios se guardan en la venta-na de eventos. En este apartado hemos resumido algunos errores típicos, sus causas y una lista de comprobaciones para los casos en que se produzca al-gún problema.

Acceso denegado

Si en la ventana de eventos se muestra el error: "Acceso denegado" para el servicio de duplicación de

directorios, verifique si este servicio está real-mente registrado con la cuenta de usuario instalada y si esta cuenta de usua-rio está disponible para los servidores de exportación e importación. Tenga en cuenta también, que el servicio de duplicación de directorios tiene acceso total a los archivos del directorio de exportación. Si el servidor d e importa-ción sólo puede leer los archivos, los enviará también con este atributo al servidor de importación, ya que aquí se utiliza el mismo acceso de usuario. En este caso, el servidor de importación no puede escribir (duplicar) los da-tos y se produce, por lo tanto, el error.

Exportación a determinados ordenadores

Si los datos sólo se pueden exportar a unos servidores de importación deter-minados, preste atención para que en las propiedades de la duplicación de directorios no se especifique el dominio correspondiente.

Autorizaciones erróneas en el directorio de importación

No modifique las autorizaciones del directorio de importación con *el Explo-rador*, ya que de hacerlo así, dejará de funcionar el servicio de duplicación de directorios.

Exportación e importación a través de una conexión WAN

Si el servicio de duplicación de directorios se realiza a través de una red de área extendida en la que los datos se distribuyan mediante determinados pro-tocolos, no será suficiente con indicar el nombre del dominio remoto para exportarlos a todos los servidores de importación. En este caso, se tiene que indicar por separado cada ordenador del dominio remoto.

Lista de comprobaciones en caso de error durante la duplicación

¿Es la cuenta de usuario del servicio de duplicación de directorios miem-bro del grupo de operadores de seguridad?

¿Se inició el servicio de duplicación de directorios en el servidor de ex-portación y en todos los servidores de importación?

¿Se encuentran el servidor de exportación y los servidores de importación en el mismo dominio? ¿Coinciden los nombres de usuario y las contraseñas?

¿Existe una relación de confianza entre los distintos dominios?

¿Se han establecido correctamente las autorizaciones para el directorio de exportación (sobre todo, y muy importante, para los directorios NTFS)?

¿Tiene el grupo local de duplicación acceso total a este directorio?

¿Está abierto permanentemente algún archivo en el directorio de expor-tación con lo que, consecuentemente, no se podría exportar nada?

¿Utilizan varios servidores de exportación de un dominio el mismo nom-bre para archivos y/o subdirectorios del directorio de exportación, con lo que se estarían sobrescribiendo mutuamente sus datos?

¿Están sincronizadas las horas del sistema del servidor de exportación y de los servidores de importación? Si no fuera así, no se enviará nin-gún dato.

10.4 Concesiones de licencias

Las redes basadas en servidores no sólo sirven para la utilización conjunta de recursos y para la comunicación entre distintos ordenadores, también se utilizan los servidores para poner servicios y aplicaciones a disposición de las estaciones clientes. En este caso también son necesarias para la red las licencias que autoricen a las estaciones clientes a usar los servicios y las aplicaciones.

Información

Hace ya algún tiempo que Microsoft cambió su política de licencias. En las redes Windows NT ya no basta con poseer licencia para los sistemas operativos de las distintas estaciones clientes. Se tienen que adquirir adicionalmente las licencias de acceso para todas las estaciones clientes, que les permitan conectarse a los servidores de Windows NT.

Si los programas de aplicación se distribuyen a través de los servidores, tam-bién tienen que adquirir para estos programas un número suficiente de licen-cias de red para todas las estaciones clientes admitidas. Al mismo tiempo, la utilización adecuada de las licencias se tiene que controlar mediante los re-cursos compartidos o programas de administración de licencias. No podrá poner excusas de ningún tipo si sólo posee cinco licencias de Word y cuenta con siete estaciones clientes utilizando simultáneamente ese progra-ma. En Windows NT, *el Administrador de licencias* supone una gran ayuda para el administrador del sistema, en la tarea de supervisar las licencias. Con él se pueden administrar las licencias de los productos. Adicionalmente, se podrá administrar la licencia para la versión de Windows NT en el ordenador local con el icono *Licencia del Panel de control.*

Diferentes concesiones de licencias

Las licencias para los productos *Back−Office* constan siempre de:

una licencia de servidor, que permite la instalación del producto en un solo servidor de la red y

varias licencias de acceso para estaciones clientes (licencias *Client Access),* a las que permite la utilización de estas aplicaciones.

Para Windows NT Server, Exchange Server, SQL Server y SNA Server se pueden conceder licencias de acceso para estaciones clientes en forma de licencia por estación cliente o de licencia por servidor. La elección dependerá de la estructura de la red.

Cuando todas las estaciones cliente de la red quieran utilizar en cual-quier momento el correspondiente producto del servidor, tendrá que elegir la concesión de licencia por estación cliente y tendrá que adquirir tantas licencias como estaciones cliente operen en su red.

Si su red se compone de muchas estaciones cliente RAS, que se conectan de tarde en tarde, ofrece más ventajas la concesión de licencia por servi-dor. En este caso, no tendrá que adquirir una licencia para cada una de las estaciones cliente y así podrá reducir los costes. En realidad, no todas las estaciones cliente se podrán conectar simultáneamente al servidor y trabajar con el correspondiente programa de aplicación.

Si por el contrario, su red consta de varios servidores que ponen las aplicaciones a disposición de cada estación cliente, puede resultar más favorable la concesión de licencia por estación de trabajo. En este caso, tendrá que adquirir un determinado número de licencias de estaciones cliente por cada servidor, que no se podrán traspasar a otros servidores. Las licencias de servidor serían menos ventajosas porque la suma de licencias de servidor de los distintos servidores sería mayor que la suma de las estaciones cliente de la red.

Para las aplicaciones en un servidor se tendría que decidir por una de estas formas de concesión de licencias, pero en el caso de contar con varios servidores y para diferentes aplicaciones, se podría componer una mezcla

de ambas formas de concesión de licencias.

El ejemplo de Windows NT Server

Toda licencia de acceso para estación cliente comprende una serie de servi-cios que, por licencia, podrían utilizarse precisamente por una estación cliente. En Windows NT Server la licencia de acceso para estaciones cliente abarca los siguientes servicios básicos de red:

Servicios de archivo: compartir los archivos, directorios y soportes de almacenamiento de datos.

Servicios de impresora: compartir las impresoras de la red.

Conexiones Macintosh: servicios de archivo e impresora para ordenado-res Macintosh.

Novell NetWare: servicios de archivo e impresora para estaciones clien-te de NetWare.

Servicio RAS: acceso remoto a Windows NT Server.

El icono licencia del Panel de control

La concesión de licencias en los ordenadores locales se puede modificar en *el Panel de control* de Windows NT con la opción LICENCIA. En tal caso, en la concesión de licencia de Windows NT se puede cambiar una única vez la opción *Por servidor* por la opción *Por puesto.*

Información

Si se decide por la opción *Por puesto*, ya no podrá modificar más adelante la concesión de licencias.

Si se decidió por la concesión de licencia *Por servidor*, podrá, en tal caso, agregar licencias y volverlas a quitar. Introduzca simplemente con el botón *Agregar licencias* el número de licencias que va a añadir y confirme que posee el contrato correspondiente para tales licencias.

En el caso de que se tengan que desconectar licencias, pulse el botón *Quitar licencias.* En la lista de licencias instaladas podrá seleccionar las licencias que desee quitar.

El controlador principal de dominio duplica automáticamente las configura-ciones de licencias en todos los controladores de dominio de reserva. Este servicio trabaja con independencia de la duplicación de directorios y de otros servicios de duplicación. Con el botón *Duplicación* del cuadro de dialogo *Elegir modalidad de licencia,* podrá introducir las opciones para la duplica-ción de datos sobre la concesión de licencias.

De forma predeterminada, la duplicación se realiza siempre con el controla-dor principal de dominio como servidor maestro. Si otro servidor de una red tuviera que desempeñar esta función, tendría que indicarlo así. Especifica-rá también el intervalo de la actualización de los datos de la concesión de licencias.

El administrador de licencias

El administrador de licencias permite a los administradores controlar las li-cencias localmente desde un ordenador o remotamente, modificar las formas de concesión de licencias, crear grupos de licencias e incluir nuevos produc-tos en el administrador de licencias.

Inicie el *Administrador de licencias* desde el menú *Herramientas adminis-trativas* del menú *Inicio.* Para poder utilizar el *Administrador de licencias*, tiene que estar registrado como miembro del grupo *Administradores.*

En el primer paso de trabajo con el *Administrador de licencias,* se selecciona el dominio para el que se tengan que verificar las licencias. El *Administra-dor de licencias* permite diferentes vistas de las concesiones de licencias en cuatro fichas distintas.

Historial de adquisiciones: En la primera ficha se muestran, cronológica-mente, los productos adquiridos. Se puede ver también la fecha en que se agregaron licencias y el número de ellas, y la fecha en que se quitaron licencias.

Ver Productos: Las licencias de esta ficha están ordenadas por produc-tos. Por los iconos que preceden a los productos, se puede apreciar de un vistazo sí quedan licencias libres, si se están utilizando todas las licen-cias o si se están utilizando más licencias de las que permite el contrato de licencias.

Clientes ("Por puesto "): En este caso, se muestra una lista de los clien-tes que hayan utilizado los productos o que los estén utilizando. Aquí también se puede apreciar, mediante iconos, si el número de usuarios sobrepasa el número máximo de licencias o no.

Visor de Servidores: En esta ficha se muestran todos los servidores de dominio propios y de dominios de confianza. Al seleccionar uno de estos servidores podrá obtener y editar las configuraciones de ese servidor.

11 REDES HETEROGÉNEAS

Windows NT se utiliza poco en entornos exclusivamente Windows. Con frecuencia nos encontramos en las redes operativas ordenadores con Windows NT, Novell o Unix conectados entre sí y, a su vez, con otros sistemas como *mainframes* o Apple Macintosh. Los sistemas operativos Workstation y Server, tan diferentes entre sí, persiguen el intercambio de datos y, en su caso, permiten también la ejecución de aplicaciones. Para conseguir tal fin, tienen que utilizar protocolos de transmisión comunes. Windows NT se adapta a tales redes heterogéneas mediante la ayuda de servicios adicionales.

Windows NT puede actuar en las redes heterogéneas

como simple servidor

como servidor de una red de Windows NT que hace de gateway (pasarela, puerta, puente, .)con las estaciones clientes Windows en las estructuras de redes heterogéneas y

como estación de trabajo que va a utilizar datos de otros sistemas.

Nos ocuparemos principalmente del papel que desempeña Windows NT como servidor.

En primer lugar veremos con detalle el protocolo más importante de las re-des heterogéneas, TCP/IP. Haciendo uso de él podrá intercambiar datos tanto con ordenadores Unix como con ordenadores Apple Macintosh.

11.1 El protocolo TCP/IP

El protocolo de transporte de Internet: Transmission Control Protocol / Internet Protocol (TCP/IP) fue desarrollado en la década de los 60 por colaboradores del Pentágono con la finalidad de crear una red de ordenadores a prueba de fallos para las situaciones de crisis. Más tarde se instaló esa red, a la que se le dio el nombre de ARPANET.

El protocolo TCP/IP adquirió las propiedades siguientes (procedentes de una idea básica de marcado matiz militar):

Es un protocolo de transporte orientado a paquetes que fracciona los da-tos en bloques, que se transmiten por separado. Los distintos bloques pueden seguir vías de transmisión diferentes desde el origen hasta el destino. En el destino se recompone el paquete original de datos. Las infor-maciones necesarias para todo ello se encuentran en la cabecera (es de-cir, en la línea de cabecera) de cada uno de los paquetes de datos.

El TCP/IP es un protocolo con capacidad de encaminamiento: el requisi-to más importante para las redes WAN.

mil

El TCP/IP es seguro contra los fallos producidos en las distintas líneas de la red: los paquetes de datos se envían por líneas distintas hasta el destino, en el que se recomponen.

Con el TCP/IP se pueden conectar entre sí sistemas operativos completa-mente diferentes.

El TCP/IP se puede utilizar como plataforma para numerosas aplicacio-nes cliente−servidor que envían los datos con este protocolo; pero, además el TCP/IP también soporta otros niveles de protocolos de la aplicación.

En la década de los setenta, el Pentágono fue perdiendo interés por ARPANET. Simultáneamente, comenzaron a interesarse por ella las universidades y otros centros de enseñanza. Como consecuencia se montaron varias subredes (entre ellas, la red BITNET), a través de las cuales se comunicaban todas esas instituciones docentes. Poco a poco se fueron integrando más y más instituciones docentes, y así fue como se formó Internet. El Pentágono se retiró completamente de ese proyecto y, a finales de los 70, se deshizo de los restos de ARPANET.

Aún hoy, Internet sigue utilizando el protocolo TCP/IP.

El modelo de niveles

Los protocolos de red están organizados en niveles. Cada nivel desempeña una función determinada en la comunicación entre ordenadores. La estructura de estos niveles tiene que estar normalizada para poder encajar las distintas aplicaciones en alguno de los diferentes niveles del modelo.

El estándar para los niveles de protocolo en las redes de área extendida fue introducido por la International Standards Organization (ISO) como el modelo Open Systems Interconnection (OSI). El modelo OSI comprende siete niveles. El TCP/IP agrupa, en su definición, algunos de estos niveles en uno solo pero, en definitiva, se corresponde totalmente con el estándar OSI.

Dentro de los cuatro niveles del estándar TCP/IP, son varios los protocolos que se encargan de la comunicación entre ordenadores. Los más importantes son el propio protocolo de transporte o protocolo de control de transmisión (TCP, Transmission Control Protocol), el protocolo de datagramas de usuario (UDP, User Datagram Protocol), el protocolo de Internet (IP, Internet Protocol), el protocolo de resolución de direcciones (ARP, Adress Resolution Protocol) y el protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol).

TCP

El TCP es un protocolo de paquetes orientado a la conexión perteneciente al protocolo de Internet (TP, consulte más adelante). Su competencia dentro del transporte consiste en garantizar la secuencia adecuada y el

control de la transmisión de datos mediante sumas comprobatorias. Si durante la transmisión se perdiese o resultase dañado algún paquete, el TCP tiene que volver a incorporar el paquete a su ruta. Esto requiere la inclusión, en cada paquete, de numerosas cabeceras que tienen que contener siempre toda la información necesaria para la recomposición de los datos fragmentados. El TCP requiere al ordenador receptor para que envíe la confirmación de la recepción correcta de los datos. En realidad se tiene que enviar una confirmación por cada paquete que haya llegado completo.

UDP

UDP es un protocolo de transporte sin conexión, con menos configuraciones de seguridad que el TCP. Los protocolos de transporte sin conexión no esperan a la indicación del terminal remoto de que se ha establecido la conexión, sino que envían sus paquetes sin más. Los paquetes de datos se envían sin sumas comprobatorias y el receptor no confirma la correspondiente recepción de los datos. Como consecuencia, los paquetes de datos son más pequeños, y la transmisión, más rápida. Por ello, el UDP sólo se puede utilizar en redes seguras en las que no se produce ningún (o apenas ninguno) error de transmisión.

IP

Este protocolo trabaja como un auténtico "mensajero dentro del protocolo antes descrito. Como protocolo sin conexión se encarga sólo del transporte de los datos, desconociendo toda corrección de errores y todo control de la secuencia de los paquetes de datos. El IP comprueba únicamente la corrección de la cabecera del paquete IP.

ARP

Este protocolo es invisible para el usuario, pero desempeña una función muy importante en el transporte de datos. El ARP determina por medio de difusiones (en inglés: broadcasts, mensajes a todos los ordenadores de la red), dónde se encuentra físicamente la dirección IP del destino de los datos. En colaboración con encaminadores, puentes y conmutadores, el ARP es el responsable de que el paquete llegue a su destino. Para averiguar las direcciones IP, el ARP envía una serie de preguntas a la red y queda a la espera de las respuestas ARP.

ICMP

Con este protocolo los ordenadores de una red TCP/IP intercambian informaciones y mensajes de error. Por lo tanto, no es responsable del transporte de datos como tal, pero garantiza la comunicación entre los ordenadores. El ICMP se utiliza, entre otras acciones, para comprobar la conexión con un ordenador remoto por medio del comando *ping*.

El servicio TCP/IP instala estos niveles en Windows NT en la arquitectura de la red Windows NT. En este caso, la *Transport Driver Interface* (TDI) actúa de mediadora entre los protocolos de transporte de TCP/IP (consulte lo anterior) y el controlador de tarjetas de red *Network Device Interface Specification* (NDIS).

En el apartado siguiente se muestra la forma de direccionar los distintos ordenadores de las redes TCP/IP.

Direcciones IP

Las redes TCP/IP se emplean tradicionalmente para conectar entre si ordenadores muy alejados unos de otros. La WAN más conocida con protocolo TCP/IP es Internet. Ésta conecta, en la actualidad, más de 40 millones de ordenadores en una red universal.

Para poder direccionar inequívocamente los ordenadores de tales redes, se tiene que contar con un sistema

normalizado de nombres o de otras denominaciones para esos ordenadores.

Las redes TCP/IP utilizan dos métodos para poder acceder a los ordenadores de la red:

Todo ordenador posee un número inequívoco en toda la red.

Se puede acceder a los ordenadores y subredes mediante el sistema de nombres de dominio (Domain Name System, DNS).

Las direcciones IP de una red TCP/IP tienen que desempeñar las funciones siguientes:

Para poder direccionar inequívocamente los ordenadores de la red, sus direcciones sólo se podrán conceder una sola vez.

A las subredes se tendrá que acceder por medio de tales direcciones o subconjuntos de una dirección.

El formato de la dirección tiene que permitir una numeración lo suficientemente amplia como para poder abarcar una gran cantidad de ordenadores (ya que el protocolo TCP/IP se usa en la red universal Internet).

En las redes locales aisladas se utiliza con frecuencia, para tal fin, el número de la tarjeta de red. Dado que ese número es único (en las topologías de redes normalizadas), se puede utilizar para la identificación de un ordenador.

En vista de que las redes TCP/IP se diseñaron, precisamente en Internet, para comunicar ordenadores remotos, la utilización de los números de tarjeta resulta inadecuada. En tal caso, hay que pensar, por tanto, en otro sistema.

Todo ordenador se identifica por un número binario de 32 posiciones. Esto es, un número formado por 32 unos y ceros. Con este procedimiento se pue-den designar, 2 elevado a 32, ordenadores y otros dispositivos distintos o, lo que es lo mismo, más de cuatro mil millones de dispositivos.

Se decidió que los nombres fueran números binarios porque estos son fácilmente inteligibles por los ordenadores. Las personas estamos más familiarizadas con el sistema decimal, por lo que el "inventor" de las direcciones IP también pensó en otra forma de escritura.

El número binario de 32 posiciones se agrupa en cuatro bloques de números binarios de 8 posiciones (=1 byte).

Cada uno de estos bloques representa un número decimal entre 0 y 255. En la notación decimal, los distintos bloques se separan unos de otros con un pun-to.

Por ejemplo:

192.171.43.12

Para el ordenador, este número tiene el siguiente aspecto:

11000000 10101011 00101011 00001100

Con esta dirección IP se puede designar un único ordenador (los denominados hosts) o un grupo de ordenadores (redes parciales, subredes). A cada uno de los dispositivos de las redes TCP/IP, se le asigna siempre una dirección IP completa en la que ninguno de los bloques es cero. Las direcciones de las subredes

comienzan por el número que comparten todos los ordenadores que componen la subred y va seguido de ceros.

Se pueden distinguir, por tanto, tres tipos de subredes diferentes que pueden incluir muchos ordenadores distintos:

Si coinciden los tres primeros bloques de números, la red puede dar cabida hasta a 254 ordenadores. En tal caso, se habla de redes de clase C.

Si coinciden los dos primeros bloques de números, la red puede contener hasta 65.534 ordenadores. Se trata, en este caso, de una red de clase B.

En las redes de clase A coincide únicamente el primer número con lo que se pueden designar más de 16 millones de ordenadores.

No todos los números se pueden utilizar en la primera posición de las direc-ciones IP de las tres clases diferentes de redes. El final del primer número se reserva para indicar la forma de la red en cuestión. Esto facilita enormemente el envío de datos en las redes TCP/IP. En la tabla siguiente le resumimos las "reglas" utilizadas en las diferentes clases de redes.

En esta tabla se supone que la dirección IP se representa mediante los números w.x.y.z.

Clase	**W**	**Dirección de la red**	**Dirección del host**	**Cantidad máxima de redes**	**Número de red ordenadores por red**
A	1−126	w	x.y.z	126	16.777.214
B	128−191	w.x	y.z	16.384	65.534
C	192−223	w.x.y	z	2.097.151	254

Quizá haya observado que el número w no puede tomar el valor 127 y que los números superiores a 223 están "prohibidos". Las direcciones 127.x.y.z se denominan direcciones *1oopback* y se utilizan dentro de la red con fines comprobatorios y de configuración. Las direcciones que posean un w superior a 223, se utilizan en las redes TCP/IP para actividades de administración y son, por lo tanto, tabú para ordenadores y subredes normales".

-

Otras direcciones se encargan de determinadas tareas y, por lo tanto, no es-tán disponibles para ordenadores u otros dispositivos en redes TCP/IP:

224 − 254 − Direcciones clase D+E

Omisiones:

0.x.y.z = para difusiones antiguas

127.x.y.z = para LoopBack (ver arriba)

255.x.y.z = para difusiones

De igual forma, tampoco se permite que ciertos números pertenecientes a los bloques de números restantes sean asignados a los ordenadores. Así, el nú-mero 254 se utiliza para el denominado gateway predeterminado,

esto es, la dirección por medio de la cual se conectan todos los ordenadores restantes de esta subred.

Para las subredes se determinan las denominadas máscaras de subred. Estas son unas direcciones IP específicas, por medio de las cuales se puede saber inmediatamente la clase de red de que se trata. En primera instancia parece que las máscaras de subred son superfluas, ya que las distintas clases de red también se pueden reconocer por el primer número de la dirección IP.

Dado que un ordenador no puede comparar simplemente si una dirección TCP/IP se encuentra en su subred, necesita la dirección de la máscara de subred. En la comunicación con ordenadores remotos añade a su dirección TCP/IP (por ejemplo, 130.100.100.85) la máscara de subred (por ejemplo, 255.255.0.0) obteniendo así 130.100.0.0. Sumando la dirección TCP/IP de un ordenador remoto (por ejemplo, 130.200.100.85) y la máscara de subred correspondiente (por ejemplo, 255.255.0.0) se obtiene 130.200.0.0. Puesto que 130. 100.0.0 es distinto que 130.200.0.0, y por lo tanto los ordenadores se encuentran en distintas subredes, el ordenador no puede establecer ninguna conexión con el ordenador remoto.

Pero en las redes TCP/IP, las máscaras de subred posibilitan otras funciones como el direccionamiento de segmentos de red.

Sólo existen tres máscaras diferentes de subred (el mismo número precisa-mente que de clases de red):

las redes de la clase A utilizan la máscara 255.0.0.0

las redes de la clase B utilizan la máscara 255.255.0.0 y

las redes de la clase C utilizan la máscara 255.255.255.0.

En este caso, el 255 sólo indica la posición de la dirección IP que comparten los distintos tipos de subred. El lugar de los ceros será ocupado por todos los números que se pueden asignar dentro de una subred.

Las relaciones existentes entre las distintas clases de redes se entenderán mejor con un sencillo ejemplo.

Un ejemplo

Un ordenador con dirección IP 134.75.69.123 se encuentra en una red cuya dirección es 134.75 y, dentro de la red, posee la dirección de host 69.123. La máscara de subred es, en este caso, la 255.255.0.0; se trata pues de una red de la clase B.

Información

En las configuraciones de los distintos ordenadores de una red utilice siempre la misma máscara de subred y las mismas direcciones de red. En caso contrario, surgirán problemas al acceder a los ordenadores y al enviar los datos (encaminamiento, consulte

más adelante). Estos problemas pueden aparecer también cuando un único ordenador utilice entradas erróneas.

11.2 Transmisión de paquetes IP: encaminamiento

En el apartado anterior se ha visto la forma de designar los ordenadores de las redes TCP/IP. Las direcciones IP garantizan la unicidad del origen y del destino en el envío de los datos. No obstante cabría preguntarse, ¿cómo se determina el camino que tienen que seguir los datos? Los encaminadores son los postes indicadores de las redes TCP/IP que determinan correctamente el desplazamiento de los datos a través de todas las "encrucijadas de caminos.

0 dicho de otro modo: los aparatos que hay en los extremos de la red TCP/IP en realidad son "tontos". Necesitan los encaminadores, que les muestran cuál es el aspecto de ese "gran mundo".

Encaminamiento: resumen Esquemático

La cabecera (header) de todo paquete de datos TCP/IP, contiene la dirección IP del origen y del destino. En su caso más simple, los encaminadores contienen una tabla de direcciones IP de subredes e informaciones, sobre la for-ma en que hay que enviar los paquetes de estas subredes. Por lo tanto, un paquete de datos que ha pasado por un encaminador puede:

enviarse a una red local si pertenece a esta subred

enviarse por medio de un (otro) adaptador de red a otra red que también disponga de encaminador o

ser rechazado por el encaminador si éste carece de información sobre la forma en que hay que volver a enviar el paquete.

Cuando un encaminador recibe un paquete de datos, utiliza en primer lugar la dirección completa para tomar su decisión. Si no encuentra en ella ningu-na relación, se van suprimiendo detalles poco a poco.

Si la tabla de encaminamiento contuviese precisamente una entrada para la dirección IP, se enviaría el paquete a ese ordenador de la red local (la denominada ruta del host).

Si no coincidiese totalmente ninguna dirección IP, se suprime la dirección del host y se empieza a buscar una subred (por ejemplo, la red 135.75.213 si la dirección buscada era la 135.75.213.12). En este caso se trata de una ruta de subred.

Si tampoco pudiera encontrarse ninguna coincidencia, se sale de la ruta de subred y el encaminador explorará únicamente la dirección de red del paquete. Se trata de la ruta de red.

Si tampoco coincidiese con ninguna entrada de la tabla de encaminamiento, el paquete se volverá a enviar a través del gateway prede-terminado, o sea, a través de la salida y entrada predeterminadas de la red en la que se encuentre el encaminador.

Si no se pudiese acceder al gateway predeterminado, se rechazará el pa-quete de datos.

Windows NT Server se puede utilizar también como encaminador de una red TCP/IP. ¿De qué forma? Eso es lo que le mostraremos en el apartado siguiente.

Encaminamiento en Windows NT

Windows NT se puede usar como un auténtico encaminador multiprotocolo desde la versión 3.51 (Servicepack 3). Con él se pueden enviar datos a otro ordenador o subred que, con distintos protocolos, haya obtenido Windows NT Server. Para efectuar esa transmisión, Windows NT podrá utilizar todos los protocolos con capacidad de encaminamiento (es decir, TCP/IP e IPX).

En este caso, describiremos el encaminamiento en TCP/IP.

Para efectuar el encaminamiento, Windows NT se vale del protocolo de in-formación para encaminamiento (RIP). Con este protocolo se pueden enviar datos IPX y datos IP. En este caso, presentaremos las funciones de encaminamiento de Windows NT, poniendo un ejemplo del encaminador IP estático. Pero Windows NT, en combinación con el servicio de servidor DHCP y el agente de reemplazo DHCP, se puede utilizar también

como encaminador dinámico (como, por ejemplo, en la transición de una red RAS a una LAN).

Con el encaminador dinámico se pueden modificar las rutas para los paquetes de datos con un número determinado (porque otra estación cliente de la red haya obtenido ya ese número por DHCP). Por el contrario, las tablas de encaminamiento estáticas no se pueden actualizar continuamente.

Para utilizar Windows NT como encaminador IP estático se tiene que activar el servicio de encaminamiento en las configuraciones TCP/IP y, a continuación, editar la tabla con los datos de encaminamiento. Realizará la primera acción con la configuración de red y, la segunda, por medio de la línea de comandos.

Activar encaminamiento IP

Dentro del *Panel de control* de Windows NT pulse el icono *Red*.

Entre en la ficha *Protocolos* y solicite en ella las propiedades del protocolo TCP/IP.

Dentro de las propiedades TCP/IP pase a la ficha *Encaminamiento* y seleccione la transmisión de paquetes IP.

Cierre los cuadros de diálogo.

Con este paso no ha terminado aún de convertir su servidor Windows NT en un encaminador. Windows NT necesita más información sobre cómo y a qué direcciones tiene que enviar. Para esto, Windows NT utiliza unas tablas de encaminamiento que se modifican desde la línea de comandos.

Edición de las tablas de encaminamiento

Para efectuar el envío de paquetes IP, Windows NT hace uso de las tablas de encaminamiento estáticas.

Estas tablas de encaminamiento contienen las columnas Dirección de red, Máscara (de subred), Gateway, Interfaz y Métrica.

Dirección de red: esta es la dirección IP del host y de la red o subred para la que es válida la entrada, esto es, para el destino de un paquete de datos IP. En esta celda pueden aparecer también direcciones IP específicas como la dirección *multicast* 224.0.0.0. Esta dirección se utiliza a efectos de administración para, por ejemplo, direccionar simultáneamente muchos ordenadores.

Máscara: la máscara de subred designa el tipo de red (clase A, clase B o clase C). Con ella se determina qué áreas de la dirección IP del paquete IP tienen que coincidir con la dirección de la red de esta entrada.

Gateway: esta es la dirección a la que se tienen que enviar los paquetes. Esta dirección podrá ser la dirección del adaptador de red local o la de otro *gateway* de la red local.

Interfaz: esta es la dirección IP de la tarjeta de red a través de la cual se tienen que enviar los paquetes.

Métrica: se refiere a la cantidad de los restantes encaminadores o esta-ciones de conmutación existentes hasta el destino. De esta forma, el encaminador podrá encontrar la ruta más rápida para los paquetes IP.

Para editar y mostrar la tabla de encaminamiento se utiliza el comando route.

Route [−f] [−p] [Comando] [Destino] [MASK Máscara de la red] [gateway] [METRIC Cantidad]

El modificador −f borra todas las entradas de gateways existentes en las ta-blas de encaminamiento.

El modificador −p instala una entrada de encaminamiento, agregada con el comando Add, de forma que ésta se mantenga incluso después de haber vuel-to a iniciar el ordenador. Si no se pone este modificador, al iniciar de nuevo el ordenador se suprimirían todas las entradas de encaminamiento.

Se dispone de los comandos siguientes:

print : imprime la tabla de encaminamientos

add : agrega una ruta a la tabla de encaminamientos

delete : elimina una ruta

change modifica una ruta existente

Los parámetros restantes modifican directamente las columnas de la tabla de encaminamientos descritas anteriormente, por lo que no se describirán en este apartado.

Para agregar una entrada de encaminamiento con la que se acceda a la subred 195.75.213.0 a través del gateway 195.75.213.254 y para lo que se necesitan dos estaciones, se compondrá el comando siguiente:

route add 195.75.213.0 mask 255.255.255.0 195.75.213.254 metric 2

En el próximo apartado le presentaremos otro servicio TCP/IP: la adjudicación dinámica de direcciones IP con el Dynamic Host Configuration Protocol.

11.3 Asignación de direcciones IP: el servidor DHCP

Dado que en las redes TCP/IP las direcciones IP tienen que ser únicas, tales direcciones no se pueden adjudicar arbitrariamente en redes TCP/IP de ámbito mundial como Internet. Para estos casos, existen instancias que supervisan la correcta adjudicación de direcciones IP. La instancia que desempeña tal función en Internet es el Centro de información de Internet (*Internet Network Information Center −InterNIC*, http://www.internic.net).

Cuando consigue una conexión Internet por medio de algún proveedor de servicios de Internet, se le adjudica una dirección IP fija, o bien el proveedor le adjudicará una dirección IP cada vez que inicie una sesión.

En el primer procedimiento, el proveedor ha solicitado previamente a InterNIC un espacio de direcciones que irá distribuyendo entre los usuarios. El encaminador del proveedor envía los paquetes de datos a los distintos clientes. Cada cliente se registra con su dirección IP determinada y se introduce en el servidor de nombres.

En el segundo procedimiento, el proveedor posee un conjunto de direcciones IP disponibles; cuando algún cliente vaya a entrar en la red, le adjudicará una dirección cualquiera de ese conjunto. Después de lo visto, es fácil hacerse la pregunta de, ¿Por qué es bueno este procedimiento (tan complicado)?, la respuesta es la siguiente:

Las direcciones IP cuestan dinero y escasean en Internet. Apenas se lo puede uno imaginar a la vista de los más de 43 mil millones de ordenadores, pero las direcciones IP se van agotando lentamente. Si el proveedor de servicios de Internet no proporciona una dirección IP propia a cada cliente, podrá sacar provecho de la circunstancia de que no todos los clientes entran en la red simultáneamente. De este modo, necesitará menos direcciones IP que clientes tenga.

Para que, a pesar de todo, siga funcionando el direccionamiento en Internet, se tiene que proporcionar un

servicio específico que asigne a los clientes direcciones IP y administre cuándo un determinado cliente ha recibido una dirección IP dada. El desempeño de esta función queda garantizado por el protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). Windows NT soporta el protocolo DHCP mediante un servicio propio. Por tanto, Windows NT puede asignar dinámicamente a los clientes de la red TCP/IP, direcciones pertenecientes a un espacio de direcciones determinado y administrar esas direcciones.

Las direcciones DHCP se editan con el administrador DHCP. En ese caso, se selecciona un servidor DHCP de la red local y se introduce para ese servidor una lista de las direcciones IP disponibles. El servidor distribuye éstas al ordenador, que realiza una consulta DHCP.

12. WINDOWS NT 4.0 EN LINEA

Conceptos como Internet o servicios en línea eran prácticamente desconocidos hace 3 años mientras que hoy no puede concebirse el marketing de nuevo software sin ellos. Windows 95 ya integró nuevas herramientas de comunicación en el sistema operativo que hasta entonces sólo estaban disponibles como programas *shareware* adicionales. Los clientes de módem, fax o correo electrónico se están haciendo tan naturales como los de impresoras.

12.1 Introducción

Como introducción a este capítulo le mostraremos una panorámica de la diversidad de herramientas de comunicación de Windows NT 4.0:

Instalación y empleo de módems: Sólo es necesario instalar y configurar una vez el módem para que lo tengamos a nuestra disposición en todas las aplicaciones. Con *HiperTerminal* y el *Marcador telefónico* podemos conectar ordenadores entre sí y establecer conexiones telefónicas.

MS Exchange: Este cliente de información universal soporta correo electrónico desde y hacia todas las aplicaciones que utilizan servicios MAPI: sistemas de correo en redes LAN como Microsoft Mail, Internet Mail y Microsoft Network. Los mensajes de los grupos de trabajo o de cualquier otro servicio de información (correo electrónico, servicios en línea) se recogen una vez recibidos o antes de ser enviados en una oficina de correos donde los podrá organizar y clasificar de forma muy intuitiva en las carpetas que establezca. Una libreta de direcciones que puede integrar las libretas de direcciones de las respectivas aplicaciones facilita la búsqueda en los diversos servicios.

MS Fax: Una vez instalado este cliente, su ordenador poseerá las capacidades de un aparato de fax. A través de un controlador de impresora especial, MS Fax es capaz de enviar fax desde todas las aplicaciones de Windows. Con MS Fax podrá enviar documentos a un aparato de fax habitual o a otro receptor, como documento procesable a través de BFT (Transferencia binaria de archivos). Además MS Fax puede usarse como un elemento integrado de MS Exchange.

Acceso a Internet (red RAS): Windows NT ofrece todos los protocolos básicos necesarios para conectar su ordenador a Internet. Con las herramientas de acceso telefónico a redes y TCP/IP se podrá conectar a un proveedor de Internet y a través de éste accederá a la red. La herra-mienta TCP/IP junto con una tarjeta de red hace posible también la conexión directa a Internet,

En los apartados siguientes aparece la red Internet en primer plano. Le mostraremos cómo conectarse a la red con los clientes de Windows NT y el modo de empleo de otros servicios como telnet, FTP y correo electrónico.

12.2 Conexión a Internet

La red Internet une entre sí ordenadores con los sistemas operativos mas diversos a través de diferentes caminos (mediante módem, conexión RDSI, líneas directas, Ethernet, radioenlaces, etc.). Únicamente, gracias a un proto-colo unitario, pueden entenderse estos mundos informáticos tan diversos. Un modelo de capas posibilita la transferencia de datos en Internet.

La conexión física (incluyendo también las conexiones a través de radio o satélite) constituye la capa inferior. Después viene el protocolo para establece-r la conexión y controlar la transferencia de datos. El protocolo punto a punto es hoy en día el estándar habitual (de la industria) en las transferencias. Como sucesor del Serial Line Internet Protocol (SLIP), el protocolo PPP incluye una corrección de errores y posibilidades de asignar direcciones de red. Y sobre esta estructura básica, el protocolo TCP/IP construye, con el entorno unitario para los protocolos, los diversos servicios de Internet (por ejemplo: http de World Wide Web, FTP para la transferencia de datos y SMTP, Simple Mail Transfer Protocol, para enviar correo electrónico `). TCP/IP es el protocolo estándar de Internet que pone de acuerdo a los protocolos de las diferentes normas de hardware y software de las redes y hace posible una comprensión universal.

Para poder acceder a la red Internet un ordenador bajo Windows NT, son necesarios los siguientes pasos:

Si no trabaja en una red conectada a Internet, deberá conseguir una cuenta PPP o SLIP de un proveedor de Internet. Windows NT controla los protocolos PPP o SLIP a través de la red RAS.

El proveedor le comunicará las informaciones de su nueva cuenta como el nombre, la contraseña y la dirección.

Según el tipo de conexión física, deberá configurar ahora una conexión de módem, conexión RDSI o una tarjeta de red.

Configure después MS TCP/IP con ayuda de los asistentes de red. Puede instalar el protocolo TCP/IP bajo NT a un nivel de igualdad junto con otros protocolos de red corno NetBEUI, SPX/IPX o Nwlink.

Una vez instalado y configurado el acceso telefónico a redes con los da-tos sobre las direcciones IP y DNS determine la conexión de acceso tele-fónico a redes en Internet. A partir de ese momento ya podrá navegar por Internet y utilizar los servicios.

A continuación, le indicaremos con más detalle cómo instalar MS TCP/IP y cómo configurar el acceso telefónico a redes.

Instalación y configuración de TCP/IP

Abra el asistente de red desde el *Panel de control* y seleccione *Protocolos*.

Pulse Agregar y luego seleccione en la lista el protocolo TCP/IP. A continuación cierre la ventana con Aceptar. TCP/IP ya está en la lista de los protocolos de red instalados.

Modifique las propiedades de la red TCP/IP.

El protocolo TCP/IP representa la base de la conexión a Internet. Si lo ha instalado correctamente podrá establecer una conexión con el proveedor de servicios de Internet a través de la red RAS.

Le he mostrado cómo puede conectarse a la red Internet. En el apartado siguiente encontrará los servicios que puede utilizar en Internet con Windows NT. Luego le enseñaré los clientes que se distribuyen con el paquete

de Windows NT 4.0 y dónde encontrará programas shareware para obtener más aplicaciones.

12.3 Uso de los servicios de Internet

Existe gran cantidad de diferentes motivos para querer participar en Internet. Encontrará en un solo medio una enorme cantidad de información, un gran parque de diversiones y un foro de debate universal. En primer lugar daré un pequeño repaso a los servicios que le ayudarán a arreglárselas en Internet.

Correo electrónico: En Internet puede enviar y recibir correspondencia. En cuestión de segundos y a un módico precio enviará textos, documentos multimedia o archivos a un receptor, a grupos de remitentes o a buzones electrónicos de cualquier parte del mundo. Windows NT incluye en MS Exchange, un cliente de información que se hará cargo de la administración y desarrollo de su correo electrónico.

News: Los usuarios de Internet debaten en los foros de discusión (newsgroups) sobre todos los temas posibles, en comp.os.ms−windows.nt por ejemplo sobre Windows NT, o en comp.os..nis−windows.programmer sobre programación en Windows.

Telnet: Con un cliente Telnet y un terminal, iniciará su conexión en otros servidores a través de programas Internet. Windows NT dispone de una sencilla terminal cliente.

File Transfer Protocol (FTP): FTP es un protocolo para transferir ar-chivos. Con él se podrá conectar a un servidor y transferir desde allí los archivos que seleccione. Windows NT posee también un cliente FTP.

Explorador World Wide Web: Un explorador WWW puede presentar en su pantalla los documentos multimedia de este servicio. WWW es una especie de subdivisión de Internet cuyos servidores presentan conexio-nes, enlaces, de hipertexto con los que se puede llamar de nuevo a otros archivos o informaciones. El paquete estándar de Windows NT contiene MS Explorer 3.0.

Archie: Este cliente de Internet trabaja como un sistema de base de datos y le ayudará en la búsqueda de archivos en servidores FTP.

Gopher: Este servicio de búsqueda va perdiendo progresivamente im-portancia debido a una representación basada exclusivamente en signos. En Gopher las informaciones se almacenan de forma jerárquica.

Wide Area Information System (WAIS): WAIS es un servicio de búsqueda que administra un índice de archivos de texto, documentos y publicaciones periódicas.

WHO IS (WH0IS): Con este servicio de búsqueda podrá buscar per-sonas y direcciones de host en bases de datos de Internet.

En el resto del capítulo explicaré cómo utilizar los programas cliente integrados en Windows NT.

Telnet

A través de un cliente Telnet se puede conectar a un ordenador remoto y utilizar los recursos que éste ponga a disposición de los usuarios. Es posible, por ejemplo, acceder al ordenador UNIX de su empresa con un portátil con Windows NT desde su residencia de vacaciones y trabajar con el ordenador que utiliza en el trabajo, siempre y cuando tanto su portátil como el ordenador de su empresa estén conectados a Internet. Puede establecer una conexión RAS con su proveedor y desde allí dirigirse a la conexión Internet de su lugar de trabajo.

En nuestro ejemplo anterior hemos hecho a propósito referencia a un ordena-dor UNIX ya que

lamentablemente la versión de Windows NT Server no ofrece un servicio Telnet al que poder conectar nuestro cliente NT. Para solucionar este problema hay que emplear todavía programas adicionales (shareware o paquetes completos de Internet comerciales).

La explicación siguiente muestra cómo se establece una conexión Telnet con un ordenador remoto y una vez allí llamar al comando de directorio ls −1.

El paquete estándar de Windows NT Workstation y de Windows NT Server contienen un cliente Telnet con el que se puede crear una conexión telnet con un ordenador remoto. Pero se trata de un programa sencillo de Microsoft, del paquete TCP/IP para Windows 3.11, no especialmente potente.

Se puede iniciar el programa Telnet pulsando dos veces el icono del programa o escribiendo el comando telnet en la interfaz de comandos.

Trabajar en un ordenador remoto

Abra en primer lugar el programa Telnet desde la interfaz de comandos o a través del icono del programa.

Establezca en Internet una conexión con un ordenador remoto con la opción Conectar, Sistema remoto. A continuación, indique la dirección IP o el nombre del ordenador remoto con el que desea conectarse.

Confirme las configuraciones con *Aceptar* para crear la conexión.

Ahora se podrá mover dentro del ordenador remoto como si estuviera sentado enfrente de él. En nuestro ejemplo hemos indicado un comando de directorio sencillo pero también podrá iniciar por ejemplo una aplicación no gráfica como Emacs o un programa de correo electrónico (véase apartado siguiente).

Finalmente iniciamos una aplicación a través de telnet. Como debe tratarse de una aplicación no gráfica he elegido el editor Emacs. Con esta herramienta del mundo de UNIX se puede escribir, jugar, administrar citas, leer y escribir mensajes y noticias y muchas operaciones más.

File Transfer Protocol (FTP)

FTP es el representante de la transferencia de datos y archivos en Internet. Identifica el protocolo que se encarga de la comunicación entre los ordenadores participantes en la transmisión. Si posee derecho de acceso en un ordenador remoto, podrá tanto copiar archivos desde ese ordenador (download) como también enviarlos (upload). Los servidores FTP públicos ofrecen accesos anónimos (anonymous FTP) con los que se permite consultar los datos de acceso público de ese servidor y obtener archivos. Hay que iniciar la sesión en el servidor FTP con el nombre de usuario anonymous o FTP e indicar como clave nuestra dirección de correo electrónico. Este último factor proviene de los tiempos en que se podían obtener archivos vía correo electrónico.

Para poder operar con FTP se requiere un cliente FTP. Windows NT ofrece un cliente no gráfico que se inicia desde la interfaz de comandos con FTP *Nombre de host.*

Búsqueda y recepción de archivos por FTP

Inicie una solicitud de entrada.

Indique el comando *ftp nombre−de−host* para poderse conectar con el ordenador de ese nombre. También puede utilizar su dirección IP.

Después de haber iniciado la sesión en el servidor FTP, nos moveremos con los comandos de directorio por los árboles de archivos de los ordenadores remoto y local. Estos comandos son una mezcla de comandos DOS, UNIX y específicos de FTP.

Finalice la sesión con el comando *bye.*

En Internet y en servicios en línea se pueden encontrar como shareware programas de cliente FTP de muy fácil manejo que ofrecen entornos gráficos.

Con ellos se pueden mostrar y copiar archivos con el ratón o mediante botones. En la ventana de aplicación dividida en dos es posible ver al mismo tiempo la estructura de unidades de disco y directorios de su ordenador local y del servidor FTP remoto.

World Wide Web

World Wide Web (WWW) es un sistema de información multimedia global en el que nos podemos desplazar a través de hiperenlaces *(hyperlinks)* por las páginas WWW de diferentes servidores WWW. La mayoría de las informaciones están compuestas con un lenguaje estándar, el HTML *(HyperText Markup Language).* Las firmas comerciales han descubierto ya las enormes posibilidades de este nuevo medio y ofrecen sus productos por medio de entornos interactivos y servicios en línea.

World Wide Web trabaja según el principio de cliente−servidor, es decir, lee las páginas WWW de un servidor WWW con un cliente WWW, el explorador. Las páginas de la Web se envían como texto (HTML) a su programa cliente que presenta gráficamente en la pantalla el resultado de ese lenguaje.

Los elementos multimedia (imágenes o secuencias de audio y vídeo) se envían separadamente del texto y el explorador las muestra mediante visores o aplicaciones especiales.

HTML reconoce comandos de diversos formatos, comandos para insertar objetos otros que hacen referencia a otras páginas WWW.

Windows NT 4.0 incluye el explorador WWW MS Internet Explorer 3.0. A continuación le mostraremos cómo encontrar y almacenar desde la WWW informaciones sobre su nuevo sistema operativo y a recopilar en una lista las referencias (enlaces) de las respectivas páginas.

Para desplazarse dentro de la WWW sólo son precisos unos pocos elementos del explorador. En la línea de debajo de la barra de herramientas se encuen-tra la dirección de la página WWW actual en forma de URL (*Uniform Resource Locator).* Podemos indicar esta dirección de forma directa o bien dejar que lo haga el explorador a través de un hiperenlace. Dentro de las páginas presentadas es posible desplazarse con los botones *FORWARD,* adelante, y B*ACK,* atrás. Los hiperenlaces (las referencias a otras páginas) pue-den ser textos o imágenes, los reconocerá porque el puntero se convierte en una mano al colocarlo sobre ellos. Generalmente los hiperenlaces de texto están subrayados o identificados con otro color y los de imagen aparecen enmarcados.

Como cuando trabajamos con otras aplicaciones de Windows, al pulsar el botón derecho del ratón se abre un menú contextual con el que es posible visualizar una imagen o desplazarnos a otras paginas.

12.4 Servicios en línea en Windows NT

Los servicios en línea como CompuServe, T−Online o AOL ofrecen su pro-pio software de acceso a través del cual nos podemos conectar con un ordenador central o con un nodo de acceso. Se puede acceder a estos servicios por módem o por RDSI.

Si desea utilizar en Windows los servicios en línea plantéese las cuestiones siguientes, que al mismo tiempo intentaré responderle:

¿Funciona también en Windows NT el programa de conexión al servicio que hemos adquirido?

Los decodificadores de AOL, T−Online y CompuServe, con los que se ha de conectar a estos servicios funcionan todos en Windows NT 4.0.

¿Es capaz el programa de controlar las interfaces con sus propios controladores de módem y RDSI?

Una conexión por módem no es ningún problema mientras no haya otro servicio que controle el módem bajo Windows NT. Aun cuando este servicio funcionase en segundo plano (como el servicio de telefonía o la red RAS) ocuparía la interfaz y no se podría conectar con los servicios en línea. Por tanto, sería necesario interrumpir primero desde el Panel de control el servicio. Este problema se puede resolver con programas para compartir puertos COM entre varias aplicaciones.

El software de acceso de los servicios en línea utilizan su propia configura-ción de módem. Será necesario, por tanto, efectuar de nuevo todas las confi-guraciones como instalación de una central privada.

Las conexiones RDSI a través del software de acceso de los servicios en línea requieren un controlador CAPI o Fossil que se encarga de la compre-sión entre la tarjeta RDSI y el software de acceso. CAPI (Interfaz común de programación de aplicaciones) es una interfaz estándar para comunicarse con las tarjetas RDSI. Los controladores FOSSIL emulan los comandos del módem en las tarjetas RDSI de forma que las controlan como a los modems con comandos AT.

Ambos programas acceden directamente al hardware (en este caso a la tarjeta RDS1) y no pueden integrarse bajo Windows NT. Por tanto las tarjetas RDSI no son viables por el momento.

¿Es posible el paso a Internet utilizando la versión propia del protocolo TCP/ IP que usa el servicio en línea (se trata de otra versión del archivo winsock.dll)?

Las nuevas versiones del software de acceso de los servicios en línea ofrecen una conexión TCP/IP con la que es posible conectarse a Internet a través de estos servicios. En CompuServe se puede acceder directamente a las páginas de Internet a partir de la versión 2.0 de WinCIM.

Las conexiones TCP/IP de los servicios en línea requieren un control TCP/IP propio y con él un archivo winsock.dll propio que realice estas tareas bajo Windows. Sin embargo, las versiones de Winsock distribuidas en el software están programadas para Windows 95 y Windows 3.11. No instale estas ver-siones en Windows NT ya que no podrá integrar de forma óptima el protoco-lo TCP/IP en la administración de red.

Si emplea un Servicio en línea como proveedor de Internet será mejor que utilice la red RAS de Windows NT para conectarse por TCP/IP con el servicio en línea. Así también podrá usar el explorador WWW de su elección, como por ejemplo el Internet Explorer Versión 3.0 de Microsoft. Si elige este camino deberá componer los comandos de acceso para establecer la conexión con el Host. Los comandos concretos que son necesarios aquí los obtendrá de su proveedor de servicios.

Conclusión

Para una conexión vía módem se puede integrar en Windows NT 4.0 sin problemas el software de acceso de los servicios en línea de AOL, T−Online y CompuServe. En WinCIM 2.0 de CompuServe prescinda siempre de la conexión a través de TCP/IP. En caso contrario no obtendrá conexión.

Para accesos RDSI a los servicios en línea deberá recurrir a las versiones de Windows 95 o Windows 3.11. Las conexiones TCP/IP deben establecerse siempre a través de la red RAS de Windows NT y no con los marcadores del servicio correspondiente. Por el momento no es posible una conexión con

AOL a través de la red RAS.

Windows NT 4.0 aún no es compatible con Microsoft Network MSN.

13. LA BASE DE DATOS DEL REGISTRO

Los sistemas operativos almacenan todas las configuraciones en los archivos de configuración. El tipo y forma de la organización de esos archivos puede hacer la vida imposible a los administradores del sistema (concepto de muchos archivos de configuración pequeños y distribuidos) o ayudarle a localizar y solucionar con rapidez los errores y anomalías (método de uno o pocos archivos de configuración centralizados).

Por fortuna, Windows NT toma este segundo camino y en consecuencia pone a nuestra disposición, con ayuda de la base de datos del registro, un archivo de configuración unificado. No es necesario realizar cada configuración en ese archivo, sino que se pueden aplicar las herramientas de servicio que se encuentran en el menú *Herramientas administrativas* o en el *Panel de control.*

13.1 Introducción

Los antiguos usuarios de DOS y Windows 3.x recordarán, seguramente con sentimientos contradictorios, los archivos de sistema (AUTOEXEC.BAT CONFIG.SYS, WIN.INI, SYSTEM.INI, NETWORK.INI,...). Para eliminar un controlador o para buscar un error del sistema había que recorrer todos esos archivos. Por eso generalmente conocían el contenido de la mayoría de los registros. Éste ya no es el caso del registro.

Advertencia

En la base de datos del registro de Windows NT, puede configurarse todo en un único pero no hay que dejar de configurar los parámetros con sumo cuidado. Para instalar un controlador son precisos varios registros que deben concordar entre sí. No en vano, Windows NT, avisa cuando se abre la base de datos desde *Diagnosis de Windows NT*.

Información

Al contrario que en Windows 95, que junto a la base de datos del registro utiliza los archivos INI, AUTOEXEC.BAT y CONFIG.SYS, Windows NT buscará en vano estos archivos. Su contenido se ha transferido, en caso de que instale Windows NT sobre Windows 3.x, a la base de datos del registro. Únicamente para programas Windows de 16 bits, que no admiten esta transferencia, deberá buscar las configuraciones en WIN.INI y SYSTEM.INI. Ambos archivos se encuentran en el directorio de programa de Windows NT.

13.2 Conceptos de la base de datos del registro

La base de datos del registro se maneja con el programa REGEDT32 que se encuentra en el subdirectorio \SYSTEM32 del directorio raíz de Windows NT. Paralelamente se puede abrir el registro con *Diagnosis de Windows NT y* con la opción *Archivo /Ejecutar/ Editor de registro (con precaución).*

Si sólo desea explorar la base de datos, puede proteger contra escritura el registro con la *opción Opciones / Modo de sólo lectura. Así* evitará modifi-car por descuido, parámetros importantes.

Las informaciones están estructuradas jerárquicamente. Existen cinco amplias áreas para no perderse en el árbol de directorios. Éstas se muestran también en el editor en ventanas especiales. La tabla siguiente muestra una panorámica de las funciones de los diferentes subconjuntos.

Árbol	**Función**
HKEY_LOCAL_MACHINE	Es el área más importante de la base de datos. Aquí se encuentran informaciones sobre el hardware de su máquina y el software de su sistema.
HKEY_CURRENT_CONFIG	En este apartado accederá a los detalles de las configuraciones actuales de los componentes de hardware y software de su sistema.
HKEY_USERS	Este es el área de los perfiles de usuario que usa Windows NT. Después del primer inicio encontrará aquí básicamente dos perfiles: el perfil estándar de Windows NT, asignado a cada nuevo usuario, y un perfil del usuario ya presente. En nombre de usuario se muestra como una combinación de dígitos precedidos de una S., la clave de seguridad del usuario.
HKEY_CURRENT_USER	Este árbol de la base de datos del registro está estructurado igual HKEY_USERS e indica directamente el perfil recién registrado.
HKEY_CLASSES_ROOT	Este árbol es en realidad superfluo. Contiene asociaciones OLE y de archivos. Todas las informaciones de este apartado se encuentran también en HKEY_LOCAL_MACHINE.

13.3 la estructura de la base de datos del registro

La estructura del registro es jerárquica. Existen apartados, como en los archivos INI, en los que pueden definirse y agregar claves (y subclaves). A diferencia de los archivos INI, en la base de datos pueden mostrarse varios niveles.

El editor del registro está estructurado de forma similar al Explorador. Cada ventana está dividida en dos mitades. En la parte izquierda se selecciona la sección, subsección, etc. La mitad derecha muestra las secciones estructuradas en niveles cada vez más interiores así como las opciones que se pueden aplicar a la sección seleccionada. Como en el Explorador, con la opción de menú *Ver* puede optarse si mostrar ambas partes (*Ver / Árbol y datos*) o sólo una de las dos (*Ver / Sólo árbol o Ver / Sólo datos*). Para ver o modificar un registro, busque en la parte izquierda del árbol la sección deseada y pulse dos veces una clave. En un cuadro de dialogo podrá introducir los valores.

Los registros de la base de datos pueden constar de diferentes tipos de datos. Cadenas de caracteres sencillas, números binarios o claves especiales. La extensión que sigue al nombre de registro, indica el tipo de entrada que Windows NT espera recibir. La tabla siguiente muestra los datos adicionales utilizados.

Tipo de dato	**Utilidad**
REG_SZ	Cadena de caracteres sencilla. También datos lógicos como *Yes* o *No*.
REG_MULTI_SZ	Este tipo de datos puede tomar varias cadenas separadas una de otra con ceros binarios.
REG_EXPAND_SZ	Cadenas de caracteres de tamaño variable. Generalmente se encuentran aquí variables como %SystemRoot% del directorio del archivo de volcado creada después de una interrupción del sistema.

REG_DWORD	Tipo de dato binario de 4 bytes de longitud.
REG_BINARY	Datos binarios. A diferencia de los ordenadores o los periféricos, las personas no pensamos en unos y ceros. Le recomiendo que se ahorre el trabajo de editar estos archivos y modifique, en su lugar, las configuraciones con las herramientas administrativas, el programa de instalación o el Panel de control.

Al pulsar dos veces un registro, el editor de la base de datos abre la ventana de edición apropiada para introducir cadenas de caracteres, datos binarios o cadenas múltiples. Con las opciones del menú *Edición* también puede abrir el cuadro de diálogo y editar cadenas de caracteres como datos binarios (si es que también piensa en unos y ceros).

El apartado siguiente muestra con sencillos ejemplos cómo modificar los registros del sistema. Para hacer efectivas las configuraciones deberá desactivar la opción *Modo de sólo lectura. No* olvide que con registros erróneos puede hacer el sistema completamente inservible. Si ha introducido un error grave, el problema se puede subsanar. Basta con apagar el sistema e iniciarlo de nuevo con la opción "Usar la última configuración buena cono-cida". Para ello pulse durante el proceso de inicio, y en el momento apropia-do (inmediatamente cuando se muestren las palabras OS *Loader),* la <Barra espaciadora>. Windows NT recurre a una copia de seguridad de la base de datos del registro y olvida todos los cambios desde el último inicio correcto.

13.4 El registro en la práctica

Mostraré el manejo del registro con parámetros sencillos e inofensivos. También podría modificar todos estos parámetros desde los menús y cuadros de diálogo del *Panel de control* y las *Herramientas administrativas.*

Además, la base de datos del registro ofrece las ventajas siguientes:

Algunos parámetros del administrador de sistema sólo pueden configurarse a través del registro.

La base de datos almacena centralizadas todas las informaciones del sistema. Después de un bloqueo, puede restituirse en un solo paso el siste-ma por medio de la restauración del registro.

Los administradores del sistema pueden editar el registro a través de la red, sin necesidad de estar físicamente frente al ordenador (administra-ción remota de un servidor NT).

Con las herramientas complementarias del Kit de recursos de Windows NT pueden crearse programas ejecutables (scripts) que editan automáticamente el registro. De esta manera pueden modificarse de forma unificada todos los servidores de la red.

Vamos a los ejemplos prácticos. En primer lugar sustituiremos el color del marco de la ventana activa por nuestro propio color.

Modificación de colores con el registro

Abra el Editor del registro llamando directamente al programa REGEDT32 del subdirectorio SYSTEM32 o inicie el registro a través del programa *Diagnosis de Windows NT.*

Active el árbol HKEY_CURRENT−USER y la clave *ControlPanel*/ *Colors*. Windows NT espera aquí cadenas de caracteres (REG_SZ) constituidas por tres números.

Windows utiliza una tabla de colores RGB. Cada color está identificado como una mezcla de rojo, verde y azul. La intensidad de los colores básicos se indica con valores numéricos entre 0 (inexistente) y 255 (100%

del color correspondiente). Para un marco rojo por ejemplo indicaremos 254 0 0. Si desea probar, pulse dos veces en la clave de registro *ActiveBorder* e introduzca como valor 254 0 0.

Después de reiniciar el ordenador, o de acceder de nuevo, se mostrarán los marcos de ventana rojos.

Examinemos otro ejemplo, la administración de la impresora con la base de datos del registro, En todo caso, podrá efectuar todas las configuraciones desde los menús de configuración de la impresora,

Encontrará las configuraciones de la impresora en el árbol HKEY LOCAL−MACHINE que, como ya he mencionado, es el conjunto más importante. Desde aquí puede buscar el registro requerido.

Búsquedas en el registro

Abra el Editor del registro.

En nuestro ejemplo queremos buscar las configuraciones de la impresora que suponemos están en el árbol HKEY LOCAL MACHINE. Por eso activamos esa entrada y seleccionamos la opción *Ver / Buscar clave*. Escriba el criterio de búsqueda "printers".

Ahora Windows NT busca en la base de datos. No se extrañe si tarda un poco más de lo que está acostumbrado con un Pentium. El primer resultado de nuestra búsqueda es la configuración de impresora que esperábamos, en *ControlSet001*.

Para llevar a cabo la configuración en *CurrentControlSet,* desplácese hasta el lugar correspondiente de esta clave o prosiga la búsqueda hasta que esté en *CurrentControlSet.*

Abriendo el registro *Printers* obtendrá una lista de todas las impresoras instaladas (en nuestro caso sólo una impresora láser NEC). Seleccionando una impresora podrá ver los registros clave en la parte derecha de la ventana. En estos registros conocerá también los límites de la base de datos del registro.

Podrá modificar sin problemas el nombre de la cola de impresora (tipo de datos REG_SZ). Será mejor que deje tal como están los datos binarios de control de la impresora, de lo contrario podría ocasionar un serio daño.

Los errores de configuración no provocarían fallos que impidan iniciar el sistema, pero seguramente los notaría en la próxima tarea de impresora, Se-ría demasiado tarde para recurrir a la opción para restaurar la clave ya que ésta es la actual. Sólo quedaría la copia de seguridad de un registro anterior o eliminar la impresora e instalarla de nuevo, lo que en este caso resultaría muy sencillo.

En los dos ejemplos anteriores hemos ajustado las propiedades del sistema operativo Windows NT y de dispositivos periféricos con el registro. Del mis-mo modo encontrará en la base de datos del registro informaciones sobre el software instalado y podrá configurar sus propiedades.

En la configuración del software también hay que distinguir entre las configuraciones globales del árbol HKEY−LOCAL−MACHINE y las configura-ciones específicas del usuario de los conjuntos HKEY−CURRENT_USER y HKEY−USERS.

Supongamos que queremos examinar las propiedades de ortografía de Ms Access. Estas se encuentran en las configuraciones globales del árbol HKEY−LOCAL−MACHINE. Seleccione allí la clave SOFTWARE/MICROSOFT/ACCESS/7.0/SPELLER. En el primer registro se puede modificar el nombre del diccionario estándar.

HKEY_CLASSES_ROOT

Las entradas de esta clave pueden dividirse en dos grandes grupos.

Por un lado, encontramos extensiones de nombres de archivo para todos los tipos de archivos registrados en Windows NT. Estas claves empiezan con un punto (.) seguido de la extensión del archivo (normalmente de tres posiciones, por ejemplo, .DOC. Con ayuda de estas claves se distinguen unos archivos de otros y se asignan los mismos a aplicaciones.

El segundo grupo está compuesto por las denominaciones de los distintos tipos de archivos, por lo que en realidad se repiten los datos para las extensiones de archivos. Aquí se definen, por ejemplo, los menús que se presentan al pulsar con el botón derecho del ratón en un archivo registrado de ese tipo.

Algunas particularidades

En este apartado queremos echar un vistazo a algunas particularidades de esta clave. Pulse en una extensión de archivo que presente un signo de adición. En algunos archivos se muestra entonces una entrada que empieza *Shell* (por ejemplo, *ShellNew).* He aquí el significado de esta entrada:

Si pulsa con el botón derecho del ratón en el área de trabajo de Windows NT, puede crear directamente un archivo de un determinado tipo con el menú *Nuevo.* Los archivos que se muestran aquí vienen definidos por la entrada *ShellNew* del registro. Obtendrá una selección de todos los tipos de archivo cuyas extensiones contengan esta clave como entrada.

Sugerencia

Las claves *ShellNew en* realidad son claves OLE 2.0 ocultas. Por lo tanto, no inserte una clave *ShellNew cuando* no sepa con seguridad que la aplicación correspondiente es compatible con OLE 2.0 o mejor prescinda de realizar modificaciones por su cuenta en este punto.

HKEY_CURRENT_USER

En este árbol del registro encontrará configuraciones de software. Aquí puede configurar qué teclado utiliza y cómo debe mostrarse el escritorio en la pantalla.

Como el nombre de este árbol ya permite suponer, aquí siempre se modifican únicamente las configuraciones para el usuario actual. Windows NT utiliza en este árbol las configuraciones (dinámicas) para actualizar las configuraciones (estáticas) del árbol HKEY_USERS al apagar el equipo y volverlas a utilizar al reiniciar el sistema. Por lo tanto, uno puede imaginarse el árbol HKEY_CURRENT_USER como una copia de trabajo de la sección correspondiente del árbol HKEY_USERS. Si modifica o elimina por error una entrada del árbol HKEY_CURRENT_USER puede subsanar el error con la sección correspondiente del árbol HKEY_USERS.

Las entradas de HKEY_CURRENT_USER pueden comprenderse mejor por todas las entradas del registro de Windows NT. Como las configuraciones suelen tratar de la apariencia de Windows NT y de algunas aplicaciones, resulta muy fácil asignar acciones a las diferentes entradas.

A continuación dedicaremos nuestra atención a algunas entradas de este árbol.

AppEvents

En la era de los ordenadores multimedia se ha puesto de moda asignar sonidos a los distintos eventos del sistema. Esto no sólo puede configurarse con el Panel de Control, sino que también puede utilizarse el registro

de Windows NT.

Las configuraciones para los sonidos del sistema se encuentran en la clave HKEY_CURRENT_USER*AppEvents*. Esta clave contiene dos entradas importantes:

En la entrada *EventLabels* se listan todos los eventos a los que se puede aplicar un sonido.

En la entrada *Schemes* están guardados los nombres de las distintas combinaciones de sonidos con *Names*. La clave *Apps contiene una lista de todas las aplicaciones que administran eventos sonoros. En la entrada default* se esconden las configuraciones actuales.

Aquí encontrará también una lista de eventos de Windows NT a los que se les puede asignar un sonido, y en las subclaves. *Default* y .*Current*, la configuración predeterminada y la configuración actual respectivamente.

Console

Con esta entrada se describen las propiedades de las aplicaciones que precisan un símbolo de DOS. Por lo tanto, se presentan también las modificaciones que realice en el símbolo de MS−DOS en Windows NT.

ControlPanel

Esta clave del registro de Windows Nt contiene todas las configuraciones del Panel de control de Windows NT relacionadas con la apariencia personal de Windows NT para un determinado usuario.

Aquí es posible modificar, por ejemplo, las configuraciones del escritorio.

A continuación le presentamos brevemente las distintas claves:

Accessibility: aquí encontrará configuraciones para las opciones de accesibi-lidad, con las que podrá configurar funciones de velocidad y de retraso de la repetición para la pulsación del teclado.

Appearance: aquí se realizan las configuraciones del color para Windows NT. En la subclave *Schemes encontrará combinaciones de colores predeterminadas como las que puede activar en el* cuadro de diálogo *Propiedades de pantalla. Si* guarda aquí una sola clave, podrá pegarla en el registro para otro usuario, copiando fácilmente todas las configuraciones en un solo paso.

Colors: aquí se determinan los colores para todos los objetos de Windows NT. En el registro pueden realizarse más configuraciones que en el cuadro de diálogo *Propiedades de pantalla*. El registro ofrece aquí una mayor selec-ción de objetos, pudiendo determinar las configuraciones para cada uno de ellos por separado (por ejemplo, botones en tres dimensiones).

Current: aquí se guardan las configuraciones de la combinación de colores actual.

Cursors: Windows NT ofrece de forma predeterminada numerosos cursores diferentes, a los que se les puede asignar distintas acciones del ratón. Aquí puede seleccionar estos cursores.

Custom Colors: si no tiene suficiente con los colores predeterminados de Windows NT, puede mezclarlos para definir colores propios. En función de la capacidad de su tarjeta gráfica obtendrá muestras de color con píxeles gruesos o tonos perfectamente mezclados si dispone de una tarjeta gráfica con representación de colores verdaderos. Aquí encontrará las configuracio-nes para mezclar sus propios colores y, naturalmente, podrá editarlos como guste.

Desktop: esta clave guarda todas las configuraciones del escritorio (fondo, protector de pantalla,...). Con la subclave *WindowMetrics* puede modificar el tamaño de los distintos elementos de la pantalla (ventanas, botones,...).

International: aquí se establecen las configuraciones regionales de Windows NT.

IOProcs: esta clave define la DLL (Dynamic Link Library) responsable de las entradas y salidas en Windows NT. No realice modificaciones en estas configuraciones, ya que podría bloquear Windows NT.

Keyboard: aquí encontrará las configuraciones de teclado actuales. Realice estas configuraciones en el Panel de control de Windows NT con los iconos *Opciones de accesibilidad o Teclado*.

Mouse: aquí se guardan las configuraciones predeterminadas para el ratón, que también pueden modificarse con el icono del mismo nombre del Panel de control de Windows NT.

Patterns: Windows NT utiliza esta sección para guardar diseños disponibles para el fondo.

ScreenSaver.<Name>: en estas entradas se determinan las configuraciones para los diferentes protectores de pantalla. Si utiliza un protector de pantalla ajeno, sus configuraciones no se presentarán necesariamente en esta clave.

Sound: esta entrada contiene otras configuraciones para los sonidos. Sin embargo, aquí no encontrará los archivos de sonido asignados a los eventos de Windows NT.

Sounds: aquí se guarda el nombre de la combinación de sonidos actual.

Las variables del entorno DOS

En la clave *Environment* están guardadas las configuraciones del entorno DOS. Puede tratarse, por ejemplo, de la ruta de acceso para archivos tempo-rales.

Printers

En esta clave se encuentran las impresoras instaladas en Windows NT que actualmente están compartidas para el usuario actual. Aquí obtendrá solamente una lista en la que figura qué impresoras están conectadas y a que puerto. No es posible realizar aquí otras configuraciones para la impresora. Para ello tendrá que utilizar las configuraciones de hardware en el registro de Windows NT.

Software

Todos los programas de software de 32 bits que instale en su grupo de progr-amas personal de Windows NT se presentarán en la clave *Software*. La información que se muestre para un programa de aplicación dependerá totalmente del programa. Así, por ejemplo, las aplicaciones de Microsoft Office permiten configuraciones para Visual Basic for Applications, mientras que otras aplicaciones sólo muestran el número de versión.

Las entradas de la clave Software corresponden a las entradas de los archivos de inicialización WIN.INI y SYSTEM.INI, que tal vez ya conozca si ha trabajado con Windows 3.x y Windows 95.

Observe, por ejemplo, la clave *Microsoft\MS Setup (ACME)\User Info.* Aquí se presenta el nombre de usuario y de empresa al que recurren la mayoría de aplicaciones durante la instalación. Este nombre sólo puede modificarlo aquí.

UNICODE Program Groups

Algunos idiomas utilizan más de 26 caracteres. A fin de poder representarlos, el sistema UNICODE utiliza 16 bits por carácter en lugar de los 8 bits habituales. En la clave UNICODE Program Groups encontrará las aplicaciones que utilizan estas configuraciones.

HKEY_LOCAL_MACHINE

En este árbol del registro de Windows NT, encontrará información crucial para el sistema operativo sobre el hardware y el software instalado. Cada componente de hardware del ordenador que deba utilizarse en Windows NT, tiene que aparecer en este árbol. Los dispositivos que no tienen entrada aquí, no pueden utilizarse en Windows NT (el sistema operativo los ignora).

Hardware

Aquí encontrará una clave para todos los componentes de hardware utilizados por Windows NT. A diferencia de lo que ocurre en Windows 95, como las entradas de esta sección no son cruciales para el sistema operativo, en Windows NT encontrará aquí la parte esencial del registro.

Todo lo que pueda configurarse en el hardware se guarda en esta sección del registro.

El árbol Hardware contiene los siguientes subapartados importantes:

Description: este apartado guarda una descripción aproximada del ordena-dor utilizado y de los puertos de comunicaciones conectados. No obstante, aquí no se configuran los distintos componentes, sino que sólo se identifican.

Devicemap: aquí encontrará para cada dispositivo instalado, un apartado que contiene una descripción y una referencia al apartado del registro con otros controladores. Resulta especialmente interesante el apartado SCSI. Este apartado también lo utilizan algunos dispositivos y controladores no SCSI.

Ownermap: los controladores Owner supervisan la función de determinados dispositivos del ordenador, como por ejemplo, las tarjetas conectadas en el bus PCI.

Ressourcemap: cada uno de los dispositivos instalados necesita determinados recursos del ordenador (direcciones de memoria, interrupciones, direcciones E/S, canales DMA). Aquí encontrará todas las asignaciones.

Software

En la clave *Software* encontrará la información y las configuraciones de todos los productos de software instalados, entre ellos los controladores para determinados componentes de hardware del sistema (por ejemplo, el controlador de la tarjeta de red).

En la clave *Classes*, igual que en el árbol *HKEY_CLASSES_ROOT*, encontrará una lista de todas las extensiones de archivo registradas. Sin embargo, las modificaciones que realice aquí no surtirán efecto en el Explorador.

También es interesante la clave *Description.* En ella se definen las Remote Procedure Calls (RPC) de Microsoft, que se utilizan en algunos programas de instalación y en conexiones de red.

Las posibilidades de configuración de esta sección del registro son muy amplias. Así, por ejemplo, al utilizar

un controlador de ratón ajeno puede cambiar la asignación de teclas del ratón. Aquí puede trabajar con total independencia de las posibilidades de configuración que le ofrezcan el Panel de con-trol o el programa de instalación suministrado con el ratón. No obstante, lamentablemente aquí sólo puedo ofrecer algunos consejos muy genera-les, puesto que las configuraciones para cada producto de software y su ins-talación son muy distintas. Algunos productos de software sólo indican aquí el número de versión actual, mientras que otros permiten realizar numerosas configuraciones.

System

Esta clave del árbol HKEY−LOCAL−MACHINE contiene todas las configuraciones para los dispositivos y componentes identificados en el apartado *Hardware*. Como es natural, aquí también puede causar los daños más graves si realiza configuraciones erróneas. En ocasiones esto puede paralizar todo el sistema y destruir la instalación de Windows NT.

Es por ello que en todo caso debe crear una copia de seguridad del registro antes de trabajar en esta clave o realizar modificaciones en ella.

Naturalmente, la clave *System* también le ofrece algunas posibilidades de ajustar el sistema. Pase, por ejemplo, a la clave *CurrentControlSet\Control\SessionManager*. Si en ella encuentra la subclave *Known16DLLs*, significa que el sistema utiliza algunas DLL de 16 bits. Si las puede reemplazar por DLLs de 32 bits, mucho más eficaces, podrá aumentar el rendimiento del sistema.

14. CUANDO EL SISTEMA SE BLOQUEA

Windows NT es conocido como un sistema operativo muy estable. Pero hasta el sistema más estable puede bloquearse o sufrir una caída de tensión. Entonces, lo importante es restaurar el sistema y los datos. Necesitará un sistema de seguridad para todas las configuraciones del sistema y copia de seguridad de los datos. Muchos temen que Windows NT 4.0 resulte menos estable sus versiones anteriores, sobre todo a raíz del traslado de los archivos USER.EXE y GDI.EXE al *micronúcleo y con* ello integrados en el controlador "anillo 0. Si esto es realmente así deberá mostrarse, según mi opinión, en la práctica. En este capítulo le mostraré las diferentes estrategias de restauración después de un bloqueo o una caída de Windows NT.

14.1 Así se inicia Windows NT

Para poder comprender por qué ya no se inicia un sistema y qué se puede hacer para solucionarlo son muy útiles algunos conocimientos sobre el pro-ceso de inicio de Windows NT. Para que un sistema pueda iniciarse es absolutamente imprescindible:

un hardware funcional y

no debe haber conflictos de hardware.

Si no se cumplen estos dos requisitos, Windows NT no podrá estar correctamente instalado y no conseguirá poner en funcionamiento su ordenador. Las posibles causas son conflictos de interrupciones o de memoria de los componentes de hardware instalados o bien unidades y controladores del disco duro y discos defectuosos.

Primero se carga el archivo NTLDR. Este cargador de inicio de Windows

comprueba en el archivo BOOT.INI la existencia de otros sistemas operativos disponibles

identifica el hardware del ordenador (NTDETECT.COM)

lee el archivo BOOTSECT.DOS que contiene el registro de inicio para el sistema alternativo, inicio dual, de MS−DOS y Windows 95 y

procesa el archivo NTBOOTDD.SYS de inicio de unidades RDSI.

El programa NTDETECT.COM supervisa, al identificar el hardware del ordenador, los números de serie del mismo, el tipo de bus, la tarjeta gráfica, el teclado, los puertos serie y paralelo, las unidades de disco y los dispositivos de pantalla.

Después de este primer paso de inicio, se carga en cuatro pasos el núcleo del sistema operativo Windows NT y la capa de abstracción de hardware (HAL):

Carga: primero se cargan el núcleo y la capa de abstracción de hardware. Para ello se cargan los archivos de sistema del área de registro HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services. Incluyen también algunos controladores de dispositivo.

Inicialización: En el paso siguiente se cargan las variables internas del núcleo y el resto de los controladores. Se comprueba que no haya errores físicos ni lógicos en las unidades de almacenamiento.

Carga de los servicios: El programa SMSS.EXE, el administrador de sesiones, organiza todos los servicios con la opción automático.

Inicio del subsistema de Windows: En el último paso se inicializa el subsistema de Windows NT. Cuando este proceso ha terminado, puede utilizarse ya una interfaz de usuario y verá en pantalla el cuadro de entrada.

Esta secuencia de inicio le ayudará a identificar el problema de Windows NT si se muestran errores al iniciarse el sistema.

14.2 Guardar configuraciones

Aun con las medidas de seguridad más amplias, puede bloquearse un ordenador Windows NT. Si afecta a un servidor que no posee un servidor de reserva puede acarrear costes considerables.

La causa de una configuración errónea de Windows NT puede aparecer, por ejemplo, tras la instalación de un controlador gráfico y dañar todo el sistema.

En este apartado conoceremos diferentes posibilidades de recuperación y reparación del sistema.

Nueva instalación del servidor

Un método de restaurar un servidor después de un bloqueo, es instalarlo de nuevo. Con ello se anula todas las configuraciones erróneas. Pero en todas las instalaciones hay que comenzar desde cero: configurar de nuevo los accesos de usuario, reinstalar todos los dispositivos, organizar de nuevo las aplicaciones... El proceso en un servidor de red con diez o veinte ordenadores puede durar una semana. Por tanto, habrá que evitar en la medida de lo posible esta vía de rescate.

Uso de configuraciones anteriores

Windows NT almacena todas las configuraciones de dispositivos y otros componentes del sistema en configuraciones de hardware. Windows NT crea una copia de seguridad para cada configuración de hardware.

Si por ejemplo, modifica algunas configuraciones del sistema, las configuraciones anteriores se guardarán en una copia de seguridad al apagar el sistema.

Si después no puede iniciarse el sistema, podrá recurrir a esa copia de segu-ridad. Pulse para ello la barra espaciadora cuando al arrancar se muestra el texto *Pulse la barra espaciadora* para iniciar la última configuración buena conocida. A continuación podrá elegir entre usar la configuración de inicio actual, usar la última configuración buena conocida o reiniciar el equipo.

El disco de emergencia

El disco de emergencia ofrece otro método para restaurar el sistema sin tener que recurrir a una nueva instalación. Este disco contiene el registro de su sistema. Es posible restaurar el sistema usando este disco junto con los discos de instalación de Windows NT.

El disco de emergencia se crea automáticamente al instalar Windows NT. Pero en la mayoría de los casos no es suficiente con crear una vez el disco y luego dejarlo a un lado. Los ordenadores se proveen una y otra vez de nuevo hardware o se incorporan en nuevos entornos.

Información

Evidentemente cada cambio del sistema no está contenido automáticamente en el disco de emergencia que ha creado al instalar Windows NT. Por eso es necesario renovar también el disco después de toda instalación de un componente de hardware.

Para crear un disco de emergencia utilice el programa RDISK.EXE del subdirectorio *System32* del directorio raíz de Windows NT. Este programa transmite al disco la configuración del *Registro.*

El disco de emergencia no contiene datos del área de usuarios de la base de datos del registro. Si restaura el sistema con este disco, dispondrá únicamen-te de los usuarios predeterminados *Administrador* e *Invitado.* Deberá crear de nuevo el resto de las cuentas.

Información

Tampoco es motivo de alarma el hecho de no haber creado todavía un disco de emergencia. Windows NT guarda en el directorio *Repair* los datos para el disco. En lugar del disco también podrá utilizar este directorio, siempre y cuando no haya resultado dañado por el bloqueo del sistema.

Creación un disco de reparación

Inicie el programa RDISK.EXE del subdirectorio *SYSTEM32* situado en el directorio raíz de Windows NT. Le saludará el "doctor del sistema".

Pulse *Crear disco de reparación* para crear un disco nuevo y *Actualizar información de reparación* para renovar uno ya existente.

Adicionalmente, puede guardar también las configuraciones del Administrador de discos asegurando con ello los datos de las particiones. Almacene estos datos en el disco de reparación o en otro disco.

Guardar la configuración del disco duro

Abra el *Administrador de discos.*

Seleccione la opción *Partición, Configuración, Guardar*.

Cierre la opción con *Aceptar*.

Para ejecutar el disco de reparación (y el disco con la configuración del disco duro) necesitará la ayuda de los tres discos de instalación de Windows NT. El apartado siguiente muestra la forma de restaurar su sistema con el disco de reparación.

Uso del disco de reparación

Introduzca en el ordenador el primer disco de instalación de Windows NT y reinicie el sistema.

Después de introducir el segundo disco de instalación hay que decidir entre instalar una nueva versión de Windows NT o reparar archivos. Seleccione *Reparar archivos* e introduzca el disco de reparación.

Windows NT leerá los datos del disco de reparación. Después deberá introducir el tercer disco de instalación para que Windows NT pueda reparar los controladores y archivos de sistema dañados. Finalmente inserte de nuevo el disco de reparación. Windows NT comprobará la unidad de inicio C: y comunicará *Reparación terminada.* Ahora podrá reiniciar su ordenador.

14.3 Medidas de recuperación

Lamentablemente también existen casos en los que ni el disco de reparación ni la configuración de hardware pueden ser de ayuda. En esos casos deberá estructurar de nuevo el sistema o como mínimo instalar de nuevo partes de él. La experiencia le enseñará que es muy recomendable disponer de medidas de seguridad para poder salvar todos los datos importantes. El requisito para ello es realizar copias de seguridad diarias de los datos del servidor. Recomiendo crear un disco de emergencia, así como una copia de la configuración del disco duro, una vez a la semana / al mes. Ante el bloqueo del ordenador, el primer paso a seguir debe consistir en buscar una alternativa.

Esto merece la pena cuando puede determinar que el problema no se puede solucionar en unos minutos o en unas pocas horas.

Aplicación de las medidas de recuperación

Cuando se bloquea un ordenador o una red, hay que actuar enseguida con el administrador del sistema. Como en la mayoría de los casos no se trabaja en este sistema, posiblemente no ha sufrido la avería. En primer lugar hay que procurarse una visión de conjunto sobre el problema. Compruebe todos los registros de sucesos y de accesos, en caso de que se pueda acceder a ellos. Si esto no es así o ya no existen los archivos, deberá valerse de los testimonios de los usuarios.

Con relación a este problema las preguntas esenciales son:

¿Se trata de un problema de software?

¿Se han modificado configuraciones? Quizá pueda trabajar aquí con las copias de seguridad de la configuración de hardware.

¿Es un problema de hardware? En ese caso hay que empezar a probar si se puede restaurar el sistema cambiando sus componentes. Pero si resul-ta haber fallado un componente de hardware esencial como el disco duro ya no queda mucho por salvar.

Guardar datos El bien más valioso de los ordenadores son los datos. Los sistemas operativos, cuentas de usuarios o aplicaciones se pueden restaurar en un momento dado pero no es tan sencillo recuperar los datos que se han perdido. Por este moti-vo es muy importante, antes de intervenir en el sistema, comprobar si todos los datos están guardados. Compruebe también, antes de borrar el disco duro actual, si realmente se pueden leer y restaurar todas las copias de seguridad. Pregunte a los usuarios del sistema si han asegurado suficientemente su tra-bajo y examine cuándo fueron guardados por última vez el conjunto de los datos de usuarios del sistema.

Si es posible, realice una copia de seguridad actual antes de efectuar cualquier trabajo de hardware, si es preciso con un disco de inicio MS−DOS compatible con la red.

14.4 Localizar errores

Cuando Windows NT no trabaja como uno quiere es necesario descubrir el error que lo impide. Para ello pueden utilizarse toda una serie de programas adicionales.

El Diagnóstico de Windows NT

En Diagnosis de Windows NT puede obtener amplia información sobre el sistema. El programa Diagnosis de Windows NT (WINMSD.EXE) se inicia a través del menú *Herramientas administrativas.*

En Diagnosis de Windows NT es posible comprobar propiedades del sistema como las asignaciones de memoria, las interrupciones y los canales DMA. En estas configuraciones encontrará (con un poco de práctica) advertencias sobre posibles conflictos de varios dispositivos y sobre errores de configuración de los mismos.

En la búsqueda de errores es especialmente importante la ficha *Recursos.*

Esta ficha ofrece una relación de los recursos del sistema ocupados por los distintos componentes de hardware. Entre los recursos del sistema se encuentran:

IRQ: también se denominan interrupciones; a través de esta ficha de interrupciones se controla un componente de hardware. El hardware lee la ficha de interrupciones constantemente, por lo que detecta de inmediato cuándo el sistema ha accedido a ellas.

Puerto E/S: todos los componentes de hardware utilizan zonas de memoria definidas para sus entradas y salidas. Estas zonas deben comunicarse a los componentes de hardware generalmente a través de puentes o de un programa de configuración propio. El sistema operativo debe saber igualmente qué componente utiliza cada zona de memoria a fin de poder transmitir o leer correctamente las entradas y salidas.

DMA: es la abreviatura de Direct Memory Access y designa un método para acceder a la memoria de forma especialmente rápida. Para ello se dispone de distintos canales DMA, que pueden almacenar las entradas en el búfer. Cada canal puede ser utilizado únicamente por un componente de hardware.

Memoria: algunos componentes de hardware necesitan para sus controladores unas zonas de memoria muy determinadas que en parte sólo pueden estar formadas por bloques consecutivos. La utilización de este tipo de bloques de memoria se desactiva con este botón.

Dispositivos: aquí encontrará una relación de los dispositivos instalados que utilizan recursos del sistema.

Para todos los recursos consumidos pueden mostrarse también los recursos HAL. Se trata de los recursos que utiliza Hardware Abstraction Layer (HAL) que media entre el hardware en sí y el núcleo de Windows NT. No

obstante, sólo pueden conseguirse las configuraciones de HAL y encontrar errores en ellas con mucha experiencia y conocimientos del sistema.

Con una doble pulsación en un recurso puede activar información más amplia sobre el mismo. Así, en el caso de una interrupción, por ejemplo, puede enterarse de si es utilizada por un único dispositivo o si es compartida con otro dispositivo o controlador.

Para localizar errores, controle si hay dobles asignaciones de los recursos. En las tarjetas que necesitan un bloque de memoria consecutivo de determinado tamaño, verifique si realmente está disponible dicho bloque.

Si no puede encontrar por su cuenta el error en el sistema en Diagnosis de Windows NT, quizás pueda recurrir a otras ayudas para obtener esa información. Para trasladar los resultados del Diagnosis de Windows NT a otros, puede guardar e imprimir en un informe el contenido de los análisis de las distintas fichas.

El depurador de errores Dr. Watson para Windows NT

Windows NT contiene un depurador de errores propio que comunica los errores en los programas Windows NT. El depurador de errores Dr. Watson para Windows NT proporciona amplia información sobre la causa del bloqueo (direcciones de memoria afectadas, posibles causas).

También es posible iniciar directamente el depurador de errores e instalarlo para que revise un determinado programa activando el programa DRWTSN32.EXE.

Elija el comando *Inicio / Ejecutar* e introduzca el nombre de programa de Dr. Watson.

A continuación se mostrará la ventana de aplicación de Dr. Watson. En ella puede configurar dónde deben colocarse el protocolo y la salida de memoria al bloquearse una aplicación. La salida de memoria de un bloqueo de programa es especialmente interesante para los programadores de dicha aplicación, ya que de este modo estos pueden encontrar el problema con mucha más rapidez.

Los usuarios no siempre pueden sacar provecho de estos datos.

Hardware Query Tool

Otra ayuda para la búsqueda de errores puede ser Hardware Query Tool, que se encuentra en el CD de Windows NT. Esta herramienta averigua la confi-guración de hardware del ordenador que encuentra Windows NT. Luego se puede comparar esta configuración con la dotación "real. Si se constatan diferencias, significa que Windows NT no ha detectado o instalado algunos componentes o bien lo ha hecho de forma incorrecta, lo cual puede ser la causa de los problemas.

Hardware Query Tool se encuentra en el CD de Windows NT, en el directo-rio \SUPPORT\HQTOOL. Primero deberá instalarla y copiar los archivos necesarios en un disquete vacío. Para ello utilice el programa *makedisk.bat* en ese directorio.

Previamente tiene que haber dado formato al disquete. HQTOOL traslada los archivos de sistema a fin de que el usuario pueda iniciar el ordenador con el disquete y analizar el hardware.

Con ese disquete se reinicia luego el ordenador. Entonces, el ordenador se inicia desde el disquete y revisa el sistema en busca de componentes de hardware detectados. Aquí es posible elegir entre una revisión más rápida y una más extensa (comprehensive). El resultado se muestra después en una ventana. Puede guardarlo en el disquete con el botón *Save* a fin de poder utilizarlo posteriormente. Encontrará un resumen de la revisión en el archivo NTHQ.TXT del disquete.

15. HERRAMIENTAS PARA WINDOWS NT 4.0

Algunas de las herramientas de Windows NT 4.0 facilitan considerablemen-te las tareas rutinarias que deseamos efectuar o complementan las funciones del sistema operativo. Dichas herramientas aparecen como Shareware en multitud de ofertas en línea o como ampliaciones comerciales de Windows NT.

Una de estas soluciones comerciales llega directamente de Microsoft y se conoce con el nombre de NT−Ressource−Kit. En ésta, los usuarios profesio-nales encuentran una variedad de herramientas y controladores de gran utili-dad que valdría la pena incorporar de forma estándar a un sistema operativo profesional como Windows NT.

En este capítulo trataremos sobre el Ressource−Kit y sus aplicaciones.

15.1 Ressource−kit

El Ressource−Kit es una colección de programas de ayuda para el control y la administración de servidores Windows NT en dominios NT. Los escasos 40 Mbytes comprenden una colección de programas con:

una gestión de usuario para dominios Windows NT

el Administrador del servidor (Server−Manager)

Perfomance−Tools

un planificador de dominios y

programas para la instalación de los mensajes de Windows NT.

Puede encontrarlo bajo el apartado *MS−Back−Office/Windows NT−Workstation* en el CD Microsoft TechNet.

Las herramientas se instalarán directamente del CD Microsoft TechNet a sus programas e iconos.

Entre las numerosas herramientas instaladas, en este libro he decidido detallar brevemente los siguientes programas:

Command Scheduler

Command Scheduler está relacionado con el comando AT para el control del tiempo NT. En lugar de sustituir el comando AT el interior de un indicador de comandos MS−DOS por parámetros,

AT [\\Nombre del ordenador] Tiempo [/Interactivo][EVERY: Fecha [, ...]] "Comando"),

Con esta herramienta pueden introducirse los comandos para el servidor de una forma fácil y segura con herramientas de Windows. Como sucedía con el comando AT, es posible la ejecución de comandos o programas "Batch" en un sistema Windows NT en puntos definidos en el tiempo de forma interactiva o como programa "Batch".

El C2 Configuration Manager

Windows NT cumple los estándares de seguridad C2 según las directrices americanas. Sin embargo, los

sistemas Windows NT no cumplen estas directrices de seguridad desde el momento de la primera instalación, antes deben introducirse manualmente ciertos parámetros que ostenta el C2 Configuration Manager del NT Ressource kit.

El C2 Configuration Manager ayuda a su sistema a obtener las directrices de seguridad C2.

Shutdown Manager

Con Shutdown Manager pueden cerrarse de forma remota estaciones de trabajo Windows NT seleccionadas o servidores Windows NT y opcionalmente volver a iniciarlos. El usuario puede obtener un texto de aviso de hasta 127 caracteres.

15. 2 Notificaciones de Windows NT

Si observamos el visor de sucesos en el grupo *Administración y con ello* descubrimos los protocolos de seguridad, del sistema y de aplicación, nos daremos cuenta que Windows NT 4.0 protocoliza innumerables procesos:

Los mensajes notifican que:

el servicio pudo iniciarse correctamente o

que se utilizará una configuración determinada y

que existe la posibilidad de que surjan conflictos del sistema y se produzcan errores.

Tras pulsar dos veces sobre el suceso, NT 4.0 muestra una descripción detallada del mismo.

Desgraciadamente, en el visor de sucesos el usuario no recibe ninguna indicación acerca de cómo resolver un posible conflicto del sistema o un error.

En ese caso, puede resultar de utilidad la base de datos de advertencias de Windows NT que se encuentra en NT Ressource Kit y Technet de Microsoft.

En caso de que surja un problema, la base de datos de advertencias de NT, una versión run−time de la base de datos relacional MS Access, proporciona al usuario valiosas indicaciones que ayudan a solucionar el error del suceso visualizado.

La búsqueda de mensajes NT se iniciará mediante el botón *Buscar.* En el cuadro de diálogo que aparece a continuación deberá introducirse como campo de búsqueda:

el texto completo

el texto de advertencia o

la identificación de red de la advertencia del visor de sucesos.

El visor de sucesos identifica la fecha, la hora, el ordenador y el número de suceso para el cuadro de diálogo *Buscar.* Según nuestra experiencia, lo más aconsejable es introducir como criterio de búsqueda el *número de suceso* (por ejemplo, 3932).

No ponga todas sus esperanzas en la base de datos de advertencias NT. La solución a algunos errores son

métodos bastante obvios y en muchos casos poco útiles como:

vuelva a iniciar el proceso

repita el proceso

cancele el proceso o

informe al administrador del sistema.

A pesar de sus defectos, la base de datos de advertencias NT se encuentra entre la colección de herramientas de todo administrador. Con esta base de datos, el visor de sucesos de NT 4.0 será algo más transparente y quizás, en algunos casos, consiga resolver el problema siguiendo sus instrucciones.

16. OPTIMIZACION DE WINDOWS NT

Windows NT requiere un hardware con una prestaciones verdaderamente elevadas. Para que su adquisición resulte rentable, tendríamos que extraer lo menor de ese hardware. La optimización de un sistema operativo como Windows NT es, por desgracia, algo más complicado que optimizar MS−DOS o Windows 95. La razón de ello deriva de que la arquitectura de Windows NT es algo más compleja.

Pero al igual que sucede en todos los restantes sistemas operativos, Windows NT cuenta, en principio, con algunos componentes que influyen decisiva-mente en la velocidad de todo el sistema. Las tres palabras mágicas respon-sables de la velocidad del sistema base se denominan memoria, disco duro y procesador(es).

Para ejecutar aplicaciones gráficas, como CAD, sobre una estación de trabajo con Windows NT, la tarjeta gráfica también desempeña, como es lógico, un papel fundamental.

Finalmente, la velocidad de un servidor de Windows NT se puede ver también retardada por las tarjetas de red, tanto en el lado del servidor como en el del cliente, así como por la topología de la red.

En este capítulo le describiré diversos motivos causantes del escaso rendimiento del sistema y le mostraremos la forma de descubrir con Windows NT los tejemanejes de tales motivos y la manera de ponerle remedio a todo ello.

Antes de empezar quiero definir algunos conceptos que se utilizan con frecuencia en este capítulo.

Tarea o función

La palabra tarea se utiliza en la actualidad en numerosas definiciones y relaciones. En este capítulo trataré el término tarea como una función determinada o una operación del ordenador que puede constar de varias instrucciones. En una tarea, el ordenador utiliza diversos recursos (CPU, memoria, disco duro, red).

El célebre cuello de botella

El rendimiento de un sistema depende con frecuencia de un componente determinado que funciona lentamente o no funciona. Al igual que en una botella el cuello determina la rapidez con que se va a vaciar su contenido, también en el ordenador se utiliza este concepto para aludir a los componentes determinantes de su velocidad.

Un ejemplo

En realidad, la copia de un disquete depende única y exclusivamente de la velocidad de la unidad de disquetes. Da lo mismo que esa unidad esté integrada en un 386, 486 o un Pentium. La unidad de disquetes asume por lo tanto el papel de cuello de botella.

Para aumentar el rendimiento de un sistema quizás se decida por la adquisición de nuevos componentes de hardware. Para que esta compra cristalice realmente en un aumento de la velocidad, se tiene que informar previamente de cuál es en realidad el cuello de botella causante del problema. En nuestro ejemplo**,** el cambio del procesador por otro más rápido no serviría de nada; la copia del disquete sólo se puede acelerar con una unidad de disquetes más rápida y, en su caso, también ayudaría un controlador de la memoria caché.

16.1 Observación del sistema

El primer paso encaminado a aumentar la potencia de un sistema es obser-varlo atentamente. El objetivo de esta observación ha de ser el descubri-miento de los cuellos de botella mencionados anteriormente y determinar sus causas.

En esto se debería recurrir ante todo al sentido común. Si un servidor de Windows NT se utiliza, por ejemplo, como servidor de archivos y de impre-sión, se debería buscar en primer lugar en estos recursos y servicios el posible cuello de botella. Precisamente muchos de los problemas de velocidad que se presentan en los servidores de archivos se pueden atribuir al acceso al disco duro y se pueden resolver con otros discos y controladores o simplemente con la defragmentación de los discos.

En un segundo paso se utiliza primeramente una de las herramientas contenidas en Windows NT para comprobar el grado de utilización de cada uno de los componentes. En particular utilice:

el monitor del sistema para documentar en un resumen gráfico el grado de utilización de cada uno de los componentes

los diagnósticos de Windows NT para controlar los recursos utilizados

el administrador de tareas de Windows NT para controlar los procesos en marcha y las aplicaciones y su consumo de los recursos del sistema

la presentación de eventos para descubrir los manejos de las funciones defectuosas y

el monitor de rendimiento de redes para comprobar la red.

Si utiliza el kit de recursos de Windows NT, encontrará en este paquete (que, por desgracia, ha dejado de ser gratis a partir de Windows NT 3.51) otras aplicaciones con las que poder rastrear el sistema.

Todas estas herramientas le ayudarán a no adquirir prematuramente nuevos y más rápidos componentes de hardware cuando, en realidad, éstos no pueden solucionar el problema.

Un ejemplo

Si está utilizando la CPU al cien por cien, antes de efectuar la compra de otra CPU más rápida se debería intentar averiguar el causante de esa sobrecarga. Esto se puede llevar a cabo fácilmente con el monitor del sistema y el administrador de tareas de Windows NT. Si, por ejemplo, el procesador se sobrecarga únicamente durante los accesos al disco duro, porque el ordenador trabaja con discos IDE, se podrá solucionar el problema comprando un controlador SCSI rápido y el correspondiente disco, y no con la compra de otro procesador.

Las cuestiones siguientes habrán de ayudarle en la localización de los cuellos de botella de este problema:

¿Cómo puedo determinar la rapidez con que tendría que trabajar realmente una aplicación, el sistema o un componente de ese sistema?

¿Cómo puedo hacer efectivamente más rápido mi sistema?

¿Cómo puedo encontrar un cuello de botella en el sistema y cómo puedo saber cuál es exactamente el componente responsable de ello?

¿Cómo puedo conseguir el equipamiento hardware adecuado a mi campo de aplicaciones?

¿Cómo puedo llegar a saber cuándo y qué hardware tengo que actualizar?

La primera cuestión es realmente la más difícil de contestar, porque en este caso tampoco yo puedo servirle de gran ayuda en este libro. Para evaluar la velocidad de un sistema se recurre en primer lugar a compararlo con otro igual o semejante. Quizás le sirva también de ayuda la evaluación subjetiva acerca de que una u otra aplicación sea más rápida o más lenta que otra. Por desgracia, los sistemas no suelen ser exactamente iguales y las diferencias, aunque sean pequeñas, impedirán que la comparación entre sistemas concluya con éxito.

En algunas revistas podrá encontrar marcas de rendimiento para evaluar el rendimiento de los procesadores, accesos a memoria, aplicaciones y accesos a datos. Si con las marcas de rendimiento se le siguen planteando los mismos problemas, podrá someter su ordenador a la comparación objetiva con los ordenadores de prueba de los laboratorios de las revistas.

Sin estos dos medios auxiliares se encontraría realmente solo ante la tarea de evaluar su sistema.

La otras cuestiones que le he planteado se contestarán en los apartados siguientes.

16.2 Mejorando la utilización y los accesos a la memoria

La escasez de memoria es una de las causas más frecuentes de la lentitud de un sistema. Si el sistema carece de memoria suficiente, los datos se tendrán que depositar en el disco duro. Se podrá dar cuenta de ello observando el sistema y comprobando que anda "hurgando" en el disco duro cada vez que ejecuta alguna acción.

La pérdida de velocidad debida a la escasez de memoria se puede evidenciar con un sencillo e ejemplo de cálculo. En ejecutar una sentencia interna el ordenador invierte unos 100 nanosegundos; en cambio, el acceso al disco duro requiere, en función del tipo de disco, unos 10 milisegundos. Por ello, todo proceso que acceda sólo una vez al archivo de intercambio, en lugar de leer los datos de la memoria principal, tendrá que ser unas 100.000 veces más lento.

Naturalmente la respuesta lógica no tiene por qué ser: "Vaya a la tienda más cercana de informática y equipe su ordenador con tanta memoria como sea posible". Por fortuna se puede rastrear previamente el sistema en busca de las aplicaciones y servicios que requieren mucha memoria y realizar las mejoras en ellos.

En este apartado le mostraremos una serie de procedimientos con los que podrá comprobar la utilización de la memoria del sistema y podrá decidir si se tiene que adquirir más memoria para acelerar notablemente el sistema.

Utilización del archivo de intercambio

Con el monitor del sistema podrá comprobar, en principio, las necesidades de memoria del sistema. Este programa se encuentra en el menú *Herramientas administrativas (Común).*

Dentro del monitor del sistema, la fuente de datos *Páginas/seg* del objeto es una buena fuente de información. Si aumenta su valor en 10 por término medio, no ha de quedarle ninguna duda de que el cuello de botella se encuentra en la memoria. La clave radica en la expresión "por término me-dio": valores punta aislados pueden sobrepasar este valor. Ejecute esta prue-ba con las aplicaciones que suele iniciar habitualmente. Carece totalmente de sentido realizar pruebas con el sistema operativo porque carece de sobrecargas.

Como medida de seguridad, vaya registrando los valores de *Bytes disponibles. Si* este valor no disminuye considerablemente cuando aumentan las *Páginas/seg,* el problema no radicará en la propia memoria, sino en el archi-vo de intercambio de una determinada aplicación.

Controle el tamaño del archivo de intercambio. Si éste sobrepasa el tamaño inicial, será porque el archivo de intercambio estará, casi con seguridad, frag-mentado. Esta podría ser la causa de unos accesos considerablemente lentos a estos datos. En tal caso compruebe la fragmentación del archivo de intercambio (page file) con un programa de defragmentación.

Comprobación de los requerimientos de la memoria

Para comprobar las necesidades reales de memoria de su sistema podrá disponer que se registre la fuente de datos *Bytes comprometidos* del objeto *Me-moria*. Si este valor sobrepasa por término medio la memoria disponible, PROBABLEMENTE su sistema está dotado de poca memoria. A tal respec-to compruebe también los valores *Fallos y Fallos de página/seg.* Cuando el número de páginas de intercambio erróneas supera el de errores de la memoria caché, su sistema almacena demasiados datos en el disco duro y puede incurrir con frecuencia en cualquier error. En este caso, sí ha de proceder a ampliar la memoria.

Que se ha puesto poca memoria a disposición del sistema será evidente cuando el valor *Bytes comprometidos* supere el de la fuente de datos *Límite comprometido.* En este caso, su sistema exigirá constantemente más memoria de la que dispone contando con la memoria física y el archivo de intercambio jun-tos. Pero dado que en este caso se trata de un auténtico error, el sistema le documentará ese error a través de la ventana de eventos. Se le mostrará el código de error 2020, 2001 y/o 2016.

Búsqueda del causante

Si realmente dispone el sistema de poca memoria, podrá investigar quién se comporta como devorador de la memoria y si en tal caso se puede economizar memoria. Para ello necesitará un programa que pueda controlar las necesidades de memoria de una aplicación o de un servicio determinados. Esto es precisamente lo que hace el programa *PMON.EXE* Visor de procesos del kit de recursos de Windows NT. Con este programa se puede controlar fácilmente las necesidades de memoria de una aplicación determinada.

Por desgracia no todos los usuarios de Windows NT disponen del kit de recursos, que comercializa Microsoft. A partir de la versión 3.51 de Windows NT, las aplicaciones del kit de recursos han dejado de estar disponibles para ser "bajadas" gratis. Pero en este caso se puede tomar un pequeño atajo.

Inicie sólo Windows NT y haciendo uso del monitor del sistema presente la utilización de la memoria tal como se ha descrito anteriormente. Si el sistema funciona a marchas forzadas o se encuentra al límite de sus posibilidades, será porque los servicios instalados consumen mucha memoria. En tal caso compruebe de qué servicios puede prescindir.

A continuación vaya iniciando sucesivamente las aplicaciones habituales y compruebe en cada caso el consumo de memoria. También así podrá emprender la búsqueda de la aplicación devoradora de memoria,

aunque algo más circunstancialmente que con el kit de recursos de Windows NT.

¡Esto es lo que podrá hacer!

Una vez que haya descubierto que la memoria es el cuello de botella de su sistema, el paso siguiente será la adquisición de más memoria.

Cuando se precisan algunas aplicaciones o servicios determinados para las necesidades de la memoria, podrá intentar ante todo renunciar a ellos a ser posible. Los servicios que no se necesitan permanentemente se pueden iniciar a mano. Consumirá memoria sólo cuando realmente la necesite.

Las aplicaciones que no necesite permanentemente las podrá ejecutar a determinadas horas del día en las que además el sistema está ocioso. Así podrá ejecutar cómodamente por las noches, entre otras actividades, aquellos cálculos intensos cuyo resultado no tenga que estar disponible inmediatamente. Para fijar los plazos de ejecución de estos programas utilice simplemente el comando *at* en el indicador de Windows NT.

Si trabaja con Windows NT en varios ordenadores / servidores, podrá distribuir algunos servicios y aplicaciones entre varios de ellos.

Si estos posibles remedios no le sirven de gran ayuda, tendrá que ampliar la memoria del sistema. Para averiguar la cantidad óptima de memoria en que se debería ampliar el sistema, compruebe de nuevo con el monitor del sistema el tamaño máximo de memoria requerido por el sistema. Calcule además un determinado almacenamiento intermedio (para aplicaciones futuras) y obtendrá la memoria que ha de añadir.

Aumentar la memoria únicamente no es suficiente

Además de la memoria, en algunos casos puede ser necesario aumentar también la denominada memoria caché de segundo nivel. Este almacenamiento intermedio del procesador tiene que direccionar ahora una cantidad mayor de memoria RAM. Si es demasiado pequeño, puede provocar errores al leer datos en esa memoria y disminuirá el rendimiento del procesador.

La ampliación de la memoria no tiene que ir necesariamente acompañada del aumento del tamaño del archivo de intercambio, aun cuando así se lo proponga el sistema. En la mayor parte de los casos este aumento provoca la fragmentación del archivo de intercambio, ya que el disco duro se ha definido anteriormente sobre la base de otros datos. Un archivo de intercambio fragmentado es, evidentemente, mucho más lento que otro compacto.

16.3 Así se mejora el rendimiento del procesador

Un procesador puede (en función de su frecuencia de reloj) ejecutar una cantidad determinada de acciones (threads) por segundo. Si el sistema cuenta con un solo procesador y tiene que ejecutar un número determinado de acciones, se tendrán que repartir la potencia del procesador entre todas las acciones que hayan de ejecutarse simultáneamente.

Como es lógico, una aplicación de Windows no requiere continuamente potencia de procesador durante todo el tiempo que se está ejecutando. Estos tiempos de espera se denominan también estados de espera. Los estados de espera de las aplicaciones de 32 bits no sobrecargan el procesador. Algo muy distinto sucede con los programas de Winl6 o los residentes en memoria de DOS, que incluso en tales estados de espera pueden sobrecargar el procesador.

Al igual que en la sección precedente hemos desenmascarado las aplicaciones y servicios que se comportaban como devoradores de memoria, también existen programas que paralizan totalmente el procesador.

El monitor del sistema le servirá de ayuda

En la búsqueda de la utilización de la potencia del procesador le seguirá siendo de ayuda el monitor del sistema.

Con la fuente de datos *% de tiempo de procesador* registre la utilización del procesador. Si ésta se encuentra continuamente en las proximidades de la marca del 100%, podría ser el procesador el actual cuello de botella de su sistema.

Si ha detectado una elevada utilización del procesador, tendrá que encontrar el causante de esta sobrecarga. Para ello utilice, entre otros, *Herra-mientas administrativas* de Windows NT, con el que podrá comprobar la utiliza-ción del procesador en el momento de iniciar cualquier servicio o aplicación.

Pero no sólo las aplicaciones pueden sobrecargar el procesador. Algunos com-ponentes de hardware también sobrecargan el procesador con interrupcio-nes. Con la fuente de datos *Interrupciones/seg* para el objeto *Procesador,* podrá provocar la presentación de estas interrupciones en el monitor del sistema. Con más de 1.000 accesos por segundo se debería comprobar ineludiblemente la efectividad del hardware, antes de decidirse por adquirir un nuevo procesador. En este caso, los causantes podrían ser los controladores del disco duro (E)IDE o las tarjetas de red.

A tal respecto observe también la fuente de datos *Llamadas del sistema/seg* del objeto *Sistema.* En este caso se trata de las llamadas básicas al procesador por parte de los servicios del sistema Windows NT. Sólo cuando se producen muy pocas llamadas del sistema al procesador en forma de interrupciones, será cuando, casi con toda probabilidad, habrá que buscar el responsable de la sobrecarga del procesador en alguno de los componentes del hardware. En cualquier otro caso será el propio sistema el que sobrecargue al procesador.

Esto es lo que podrá hacer

En los casos de elevada utilización de¡ procesador también se podrá recurrir a otros métodos distintos al de sustituir el procesador por otro más rápido o utilizar otro procesador.

Como sucedió con los problemas de memoria, las aplicaciones menos necesarias y que sobrecargan los procesadores se podrán ejecutar sólo cuando realmente hagan falta, Numerosos cálculos se pueden ejecutar por las noches, cuando el ordenador está menos sobrecargado con los accesos de los usuarios.

Si en el ordenador con Windows NT se ejecutan programas escritos por el usuario, podrá tomar las medidas oportunas para realizar una programación "respetuosa con el procesador".

Distribuya las aplicaciones entre varios ordenadores cuando ello sea posible.

Controle la tarjeta de red de su PC. Si sigue utilizando aún alguna antigua tarjeta de 16 bits (o incluso alguna otra de 8 bits), éstas requerirán más potencia del procesador que su nueva representante de 32 bits. Por lo tanto, sustituya la tarjeta si hubiere lugar a ello. Al adquirir una tarjeta de 32 bits cerciórese de que cuenta con acceso directo a memoria (DMA). Esta tarjeta es considerablemente más rápida y sobrecarga menos el procesador.

Todo proceso en Windows NT se ejecuta de acuerdo con una prioridad determinada. Con *Herramientas administrativas* podrá asignar a cada proceso una, prioridad más baja o más alta.

En algunos casos no se tendrá que cambiar el propio procesador, sino su memoria caché. Ya le hemos descrito un caso de estos en la sección anterior.

Cuando la elección ha de recaer en la utilización de otro procesador o en la sustitución de uno ya existente por otro más rápido, podrá decidir, a la vista de las aplicaciones utilizadas, cuál de las dos opciones es la mejor. Si utiliza un ordenador con varios procesadores, Windows NT reparte los threads y las interrupciones entre esos procesadores. Así, por ejemplo, en un procesador podrá ejecutar un proceso de uso intensivo de la CPU y el otro procesador estará a su disposición para ejecutar otras aplicaciones. En esta situación, disponiendo de un único (y rápido) procesador podrían aparecer antes los conflictos. También los servidores de Windows NT que han de hacer frente a muchos accesos de clientes simultáneamente, sacarán más provecho de otro procesador que de uno más rápido.

Sin embargo, si utiliza aplicaciones de CAD o de multimedia, entre otras, en una estación de trabajo con Windows NT, obtendrá, en su caso, mejores resultados con un único procesador (MMX).

Utilización de aplicaciones de 16 bits

Las aplicaciones de 16 bits se pueden convertir fácilmente en una pesada carga para el procesador. Toda aplicación de MS−DOS se ejecuta con Windows NT en una máquina virtual de MS−DOS. Por ello, en la lista de las aplicacio-nes ejecutadas aparecen todas con el nombre de NTVDM.EXE.

Cuando no esté contento con el rendimiento de sus aplicaciones Win16 en un ordenador con Windows NT, debería recurrir en primer lugar a ejecutar estas aplicaciones en modo de pantalla completa. En este modo las aplicaciones pueden trabajar más fácilmente con sus propias rutinas gráficas y, por lo tanto, alcanzan generalmente una mayor velocidad.

Cuando sus aplicaciones Win16 utilicen el puerto COM (como, por ejemplo, para acceder a un módem), podrá acelerar los accesos al puerto haciendo uso de software (de protocolo Xon/Xoff), en lugar de hacerlo con hardware (de protocolo cts/rts). La aplicación Winl6 no puede ejecutar realmente el chequeo del hardware, ya que Windows NT tiende su mano protectora sobre todos los accesos al hardware. Recorrer este atajo puede costar un tiempo precioso.

16.4 Acelerar los accesos al disco duro

Esta última sección del capítulo la quiero dedicar a los accesos al disco duro. El disco duro es el dispositivo de entrada y salida más importante en la mayor parte de los sistemas y, por lo tanto, determina básicamente la velocidad del sistema.

En un primer paso se debería comprobar la fragmentación del disco duro. Las estructuras segmentadas de soportes de datos son la causa más simple y más fácil de solventar de la lentitud de los discos duros.

Podrá verificar el rendimiento del disco duro con el programa *diskperf −y* que, tras su introducción, solicitará un nuevo inicio del sistema para entrar en vigor. La mayor parte de los programas de verificación del rendimiento del disco duro necesitan a su vez un conjunto completo de recursos de tal forma que Windows NT no los inicia automáticamente.

Además de esta herramienta, el monitor del sistema continúa estando a su disposición, como no podía ser de otra forma. Con todo ello se podrá mostrar, por ejemplo, la fuente de datos *% Tiempo de disco* del objeto *Disco físico*. Con estas cifras podrá conocer el porcentaje de los tiempos de acceso del soporte de datos invertido por los procesos de lectura, escritura y de espera.

Con la fuente de datos *Long. promedio de la cola de lectura de disco* del objeto físico podrá además comprobar directamente cuánto tiempo tienen que esperar las operaciones de archivo al disco duro. Si la longitud de esta cola de espera supera el valor 2, el acceso al disco duro será entonces el cuello de botella.

Si ha determinado que el disco duro es el cuello de botella de su sistema, n-o podrá, en contraposición con lo sucedido con los problemas vistos hasta ahora, seguir ahorrando en hardware. En general, un nuevo controlador del disco duro o un nuevo disco duro solucionará el problema.

En este caso Windows NT le estaría muy agradecido si recurriese a un disco duro SCSI con un rápido controlador PCI−SCSI. Estos controladores pueden procesar en paralelo varios procesos de lectura y escritura incrementando así considerablemente el rendimiento, sobre todo en los entornos de servidores con gran cantidad de accesos a archivos.

Si ya trabaja con varios discos duros, podrá aumentar el rendimiento *del* sistema con un procedimiento RAID. Como es lógico necesita para ello un controlador de disco duro con capacidad RAID u otro adicional (RAID 5).

17. WINDOWS NT COMO SERVIDOR DE INTERNET

La presencia de Internet ha dejado de ser un asunto exclusivo de las grandes empresas. Aumenta continuamente el número de pequeñas empresas que se anuncian en este medio y que venden sus productos y prestan sus servicios a través de esta red. Si no desea que su oferta permanezca almacenada en algún proveedor o editorial, tiene que instalar su propio servidor para los servicios de Internet.

Windows NT 4.0 Server contiene el servidor de información de Windows. Por medio de él se puede instalar:

un servidor WWW

un servidor FTP y

un servidor Gopher.

Tales servidores utilizan las configuraciones TCP/IP asignadas durante la instalación de este protocolo de red. Tiene que garantizar, por tanto, bien mediante la instalación de este servicio, bien mediante programas adicionales específicos en NT Server, que los paquetes de Internet o de su intranet lleguen también a su destino. Para ello, puede ser necesario instalar Windows NT adicionalmente como servidor de nombres o como encamonador.

A continuación, paso a describir los tres servicios de servidor.

Servidor WWW

El World Wide Web se ha convertido en la actualidad en un boom como medio de información y de distribución. De él ya he hablado anteriormente (en el capítulo 12), y en este momento me voy a limitar ha describir la forma de instalar un servidor WWW con el propio Windows NT.

El WWW trabaja según el principio cliente−servidor. Si su servidor de Windows NT recibe una petición WWW (la denominada petición HTTP) en una dirección IP, se activará el servidor de información de Internet (si dicho servicio estuviera iniciado).

Los servidores WEB muestran una página inicial general o las páginas explícitamente solicitadas:

si se envió como URL el nombre o la dirección del ordenador sin más indicaciones, se mostrará una página inicial determinada

los clientes pueden solicitar directamente un página de un directorio compartido determinado del servidor WWW.

Windows NT organiza los servicios de Internet de la misma manera que cualquier otro servicio. Una vez iniciado el servicio, su ejecución continuará en segundo plano. Únicamente se activará cuando reciba una petición. Todo servicio se tiene que configurar minuciosamente. De esta forma, se podrá determinar y limitar el acceso al servidor WWW a los usuarios de unidades y directorios que realmente tengan autorización para acceder.

El servidor de información de Microsoft es un servidor WWW fácil de administrar, pero no excesivamente potente. Soporta pocos archivos de comando para la creación de páginas WWW interactivas; no soporta ningún archivo de comando CGI para realizar formularios, y su rendimiento no es suficiente para instalar un servidor WWW grande. El rendimiento del servidor WWW de Microsoft da, como máximo, para prestar pequeños servicios de servidor WWW o para ejercer como medio de información en una intranet.

Si desea montar en Windows NT un servidor WWW profesional y desde él ofrecer desde Internet sus informaciones, productos o prestaciones de servicios, tiene que decidirse por un servidor WWW potente para Windows NT. Algunos se pueden conseguir como shareware en condiciones muy favorables. La tabla siguiente muestra un resumen de ellos (hay que tener en cuenta que esta tabla no esta actualizada, es decir, que es muy posible que algunos de ellos ya no existan o hallan cambiado el precio y el URL).

Nombre	**Fabricante**	**Precio**	**URL**
https	EMWAC	Libre	Emwac.ed.uk
SAIC	SAIC	S/especificar	www.saic.com
GNNServer	GNN	Libre	www.tools.gnn.com
JSB INTRAnet Jazz	JSB, GB	S/especificar	www.jsb.co.uk
SuperWeb	Frontier	795$	www.frontiertech.com
FolkWeb	ILAR Concepts	120$	www.ilar.com
Spry Web Server	SRPY	245$	Server.spry.com
WebSite	O'reilly&Ass	449DM	Website.ora.com
InfServer	Microsoft	Libre aún	www.microsoft.com

Servidor Gopher

Gopher es un medio de información muy elemental (y como consecuancia muy rápido) que presenta las informaciones jerárquicamente como el índice de un libro. La gran ventaja ante el WWW estriba en el sencillo diseño de las páginas. Durante la búsqueda, ninguna imagen animada perturba la transmisión de las páginas. Pulsando las distintas jerarquías, se accede a los contenidos esperados. Estos pueden constar de los documentos más diversos, que se cargan en el propio ordenador y se muestran con algún presentador de archivos apropiado. Este servidor lo comento simplemente como curiosidad, ya que en la actualidad ya ha desaparecido de Internet.

El servidor de información de Microsoft ofrece también este servicio.

Servidor FTP

Con el protocolo de envío de archivos (File Transfer Protocol, FTP), se pueden poner los archivos a disposición de los usuarios de Internet o intranet y se pueden recibir también archivos procedentes de esas redes. En el capitulo 12 he tratado un poco más a fondo este servicio. El servidor de información de Microsoft contiene también un servidor FTP.

Los servidores FTP de Microsoft pueden

ser instalados para permitir el acceso anónimo de usuarios

admitir también como usuario FTP a los usuarios instalados en el dominio NT

poner a disposición del dominio de Windows NT la autorización de acceso con contraseña.

Si Windows NT Server es accesible desde el exterior, habría que andar con mucho cuidado. Las contraseñas se envían sin encriptar y serían presa fácil para los usuarios no autorizados que, con la contraseña del dominio en su poder, podrían acceder a otros recursos de la red.

En estos casos sirve de gran ayuda la encriptación de datos que Windows NT pone a su disposición en la versión 4.0 con su conexión PPTP entre dos servidores NT. La transmisión de contraseñas dejaría de ser insegura, siempre que se conectasen a la red usuarios de Windows NT Server o Workstation 4.0.

El elemental servicio FTP se instala con gran rapidez. Se tiene que especificar si hay que permitir accesos anónimos y los derechos de los accesos. Para ello se crea una lista de los directorios disponibles y se determina si hay que permitir el acceso de lectura o de escritura.

Al igual que sucedía con otros servicios de información de Microsoft, los servidores NT se pueden bloquear para determinados ordenadores o subredes. Para informar a los usuarios acerca de las directrices de un servidor FTP, los administradores preparan unos mensajes que sirven de información para los usuarios cuando inician su sesión o cuando se produzcan sucesos.

Tras un breve manejo de su servidor FTP, estará en condiciones de responder a través de él a las consultas de Internet.

18. COMANDOS NET

Muchos comandos de red de Windows NT empiezan por la palabra net. Estos comandos net tienen algunas propiedades en común:

Puede ver una lista de todos los comandos net disponibles si escribe *net/?*

Puede obtener ayuda sobre la sintaxis en la línea de comandos para un comando net si escribe *net help [comando]*. Por ejemplo, si desea ayuda sobre el comando *net accounts*, escriba *net help accounts*.

Todos los comandos net aceptan las opciones */yes* y */no* (se pueden abreviar a */y* y */n*). La opción /y responde automáticamente `sí' a cualquier mensaje interactivo que genere el comando, mientas que /n responde `no'. Por ejemplo, *net stop server* suele pedirle que confirme que desea detener todos los servicios que dependen del servicio Servidor*; net stop server* /y responde automáticamente `sí' al mensaje y se cierra el servicio Servidor.

Net Accounts

Actualiza la base de datos de cuentas de usuario y modifica los requisitos de contraseña e inicio de sesión para todas las cuentas. El servicio Inicio de sesión de red debe estar en ejecución en el equipo para el que desee cambiar los parámetros de cuenta.

net accounts [/forcelogoff:{minutos | no}] [/minpwlen:longitud] [/maxpwage:{días | unlimited}] [/minpwage:días] [/uniquepw:número] [/domain]

net accounts [/sync] [/domain]

Parámetros

Ninguno

Escriba net accounts sin parámetros para presentar en pantalla las configuraciones actuales de contraseña, limitaciones de inicio de sesión e información de dominio.

/forcelogoff:{minutos | no}

Establece el número de minutos que transcurrirán antes de que se dé por finalizada una sesión de usuario en un servidor tras el vencimiento de la cuenta de usuario o el tiempo válido de inicio de sesión. Con la opción no se impide que se produzca un cierre de sesión forzado. El valor predeterminado es no.

Cuando se especifica la opción */forcelogoff:minutos*, Windows NT envía una advertencia minutos antes de forzar la salida del usuario de la red. Si hay algún archivo abierto, Windows NT advierte al usuario. Si minutos es menor que dos, Windows NT indica al usuario que cierre la sesión de red inmediatamente.

/minpwlen:longitud

Establece el número mínimo de caracteres para la contraseña de una cuenta de usuario. Los valores válidos oscilan entre 0 y 14 caracteres; el valor predeterminado es de 6 caracteres.

/maxpwage:{días | unlimited}

Establece el número máximo de días de validez de la contraseña de una cuenta de usuario. El valor *unlimited* establece un tiempo ilimitado. La opción */maxpwage* debe ser mayor que */minpwage*. Los valores válidos oscilan entre 1 y 49710 días (unlimited); el valor predeterminado es de 90 días.

/minpwage:días

Establece el número mínimo de días que han de transcurrir antes de que un usuario pueda cambiar una contraseña nueva. Un valor 0 significa que no hay tiempo mínimo. Los valores válidos oscilan entre 0 y 49710 días; el valor predeterminado es de 0 días.

/uniquepw:número

Impide que el usuario repita la misma contraseña durante número cambios de contraseña. Los valores válidos oscilan entre 0 y 8 cambios de contraseña; el valor predeterminado es de 5 cambios.

/domain

Realiza la operación sobre el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local.

Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De manera predeterminada, los equipos con Windows NT Server realizan las operaciones sobre el controlador principal del dominio.

/sync

Cuando se utiliza en el controlador principal de dominio, causa la sincronización de todos los controladores de reserva de dicho dominio. Cuando se utiliza en un controlador de reserva, causa la sincronización de ese controlador de reserva con el controlador principal de dominio únicamente. Este comando sólo se aplica a los equipos que son miembros de un dominio de Windows NT Server.

Ejemplos

Para mostrar la configuración actual para el cierre forzado de sesión, los requisitos de contraseña y la función de un servidor determinado, escriba:

net accounts

Para establecer un mínimo de siete caracteres para las contraseñas de la cuenta de usuario, escriba:

net accounts /minpwlen:7

Para especificar que una contraseña no pueda repetirse hasta pasados cinco cambios, escriba:

net accounts /uniquepw:5

Para evitar que los usuarios cambien la contraseña con una frecuencia mayor que cada 7 días, para forzar el cambio de contraseña cada 30 días y para forzar el cierre de sesión tras el vencimiento del tiempo de inicio de sesión y emitir una advertencia 5 minutos antes del cierre forzado, escriba:

net accounts /minpwage:7 /maxpwage:30 /forcelogoff:5

Para realizar la tarea anterior en un equipo con Windows NT Workstation y asegurarse de que la configuración es efectiva en el dominio de Windows NT Server en el que el equipo ha iniciado la sesión, escriba:

net accounts /minpwage:7 /maxpwage:30 /domain

Para actualizar la base de datos de cuentas de usuario de todos los servidores miembros, escriba:

net accounts /sync

Net Computer

Agrega o elimina equipos de una base de datos de dominios. Este comando está disponible sólo en los equipos con Windows NT Server.

net computer \\equipo {/add | /del}

Parámetros

\\equipo

Especifica el equipo que se agrega o elimina del dominio.

/add

Agrega el equipo especificado al dominio.

/del

Quita el equipo especificado del dominio.

Notas

Este comando está disponible sólo en los equipos con Windows NT Server.

Todas las adiciones y eliminaciones de equipos se redirigen al controlador principal de dominio.

Ejemplo

Para agregar el equipo ARCOIRIS al dominio, escriba:

net computer \\arcoiris /add

Net Config

Muestra los servicios configurables que están en ejecución, o muestra y modifica la configuración de un servicio.

net config [servicio [opciones]]

Parámetros

Ninguno

Escriba *net config* sin parámetros para ver una lista de los servicios configurables.

Servicio

Es un servicio (Server o Workstation) que puede configurarse con el comando *net config.*

Opciones

Son específicas del servicio. Vea net config Server o net config Workstation para obtener la sintaxis completa.

Use el comando *net config* servicio para cambiar parámetros configurables de servicio Servidor o Estación de trabajo. Los cambios entran en vigor inmediatamente y son permanentes.

Net Config Server

Muestra o cambia la configuración para el servicio Servidor mientras dicho servicio está en ejecución.

net config server [/autodisconnect:tiempo] [/srvcomment:"texto "] [/hidden:{yes | no}]

Parámetros

Ninguno

Escriba *net config server* para ver la configuración actual del servicio Servidor.

/autodisconnect:tiempo

Establece el número máximo de minutos que una sesión de usuario puede permanecer inactiva antes de que se desconecte. Puede especificar −1 para que nunca se produzca dicha desconexión. Los valores válidos oscilan entre −1 y 65535 minutos; el valor predeterminado es 15.

/srvcomment:"texto"

Agrega un comentario para el servidor que se muestra en las pantallas de Windows NT y con el comando net view. El comentario puede tener un máximo de 48 caracteres. Escriba el texto entre comillas.

/hidden:{yes | no}

Especifica si el nombre de equipo del servidor debe aparecer al presentar la lista de servidores. Tenga en cuenta que el hecho de ocultar un servidor no modifica los permisos definidos en él. El valor predeterminado es no.

Ejemplos

Para mostrar información acerca del servidor local e impedir que la pantalla se desplace, escriba:

net config server | more

Para ocultar el nombre de equipo del servidor en la lista de servidores disponibles, escriba:

net config server /hidden:yes

Para desconectar a un usuario después de 15 minutos de inactividad, escriba:

net config server /autodisconnect:15

Notas

Utilice el comando net config server para cambiar parámetros configurables del servicio Servidor. Los cambios entran en vigor inmediatamente y son permanentes.

No todos los parámetros del servicio Servidor pueden cambiarse utilizando el comando net config server, pero el comando presenta información adicional. El comando presenta la siguiente información acerca del servidor:

El nombre de equipo del servidor, un comentario descriptivo y la versión del software.

La descripción de la red.

La configuración de ocultar el servidor.

El número máximo de usuarios que pueden utilizar los recursos compartidos del servidor.

El número máximo de archivos del servidor que pueden estar abiertos.

La configuración del tiempo de inactividad de la sesión.

Net Config Workstation

Muestra o cambia la configuración del servicio Estación de trabajo mientras está en ejecución.

net config workstation [/charcount:bytes] [/chartime:ms] [/charwait:s]

Parámetros

Ninguno

Escriba n*et config workstation* para mostrar la configuración actual del equipo local.

/charcount:bytes

Especifica la cantidad de datos que recopila Windows NT antes de enviarlos a un dispositivo de comunicaciones. Si se establece también /chartime:ms, Windows NT actúa según la condición que se satisfaga primero. Los valores válidos oscilan entre 0 y 65.535 bytes; el valor predeterminado es de 16 bytes.

/chartime:ms

Establece el número de milisegundos durante los cuales Windows NT recopila datos antes de enviarlos a un dispositivo de comunicaciones. Si se establece también */charcount:bytes*, Windows NT actúa según la condición que se satisfaga primero. Los valores válidos oscilan entre 0 y 65.535.000 milisegundos; el valor predeterminado es de 250 milisegundos.

/charwait:seg

Establece el número de segundos que esperará Windows NT a que un dispositivo de comunicaciones esté disponible. Los valores válidos oscilan entre 0 y 65.535 segundos; el valor predeterminado es de 3.600 segundos.

Ejemplos

Para presentar en pantalla la configuración actual del servicio Estación de trabajo, escriba:

net config workstation

Para establecer el número de milisegundos que Windows NT espera antes de enviar los datos a un dispositivo de comunicación a 500 milisegundos, escriba:

net config workstation /chartime:500

Notas

Use el comando net config workstation para cambiar parámetros configurables del servicio Estación de trabajo. Los cambios entran en vigor inmediatamente y son permanentes.

No todos los parámetros del servicio Estación de trabajo pueden cambiarse con el comando net config workstation. Otros parámetros pueden cambiarse en el registro de configuración.

Net Continue

Vuelve a activar un servicio interrumpido.

net continue servicio

Parámetros

Servicio

Los servicios que pueden reanudarse son los siguientes: servidor de archivos para macintosh (sólo para Windows NT Server), servicio de publicación de FTP, lpdsvc, inicio de sesión de red, dde de red, dsdm dde de red, proveedor de seguridad nt lm, inicio remoto (sólo para Windows NT Server), servidor de acceso remoto, schedule, servidor, servicios simples de tcp/ip y estación de trabajo.

Notas

En un servidor y en un cliente:

Use el comando *net continue* para volver a activar un servicio interrumpido. Interrumpa el servicio antes de detenerlo para permitir que los usuarios finalicen sus trabajos o se desconecten de los recursos. Para efectuar una corrección poco importante en un recurso, quizá sea suficiente con efectuar una pausa en el servicio o la impresora. Use después el comando *net continue* para activar de nuevo dicho servicio o impresora, sin necesidad de cancelar las conexiones de los usuarios.

En un cliente:

Use los comandos net pause y *net continue* para pasar de las impresoras de la red a la impresora conectada a su equipo.

Net File

Muestra los nombres de todos los archivos compartidos abiertos en un servidor y el número de bloqueos de archivo (si existe alguno) en cada uno de ellos. Este comando también cierra archivos compartidos individuales y quita bloqueos de archivo.

net file [id [/close]]

Parámetros

Ninguno

Escriba *net file* sin parámetros para obtener una lista de los archivos abiertos en un servidor.

Id

Es el número de identificación del archivo.

/close

Cierra un archivo abierto y libera los registros bloqueados. Escriba este comando desde el servidor en el que se comparte el archivo.

Ejemplos

Para ver una pantalla de información acerca de los archivos compartidos, escriba:

net file

Para cerrar un archivo con el número de identificación 1, escriba:

net file 1 /close

Notas

Este comando también puede escribirse como net files.

Use el comando *net file* para ver y controlar archivos compartidos en la red que, en ocasiones, se dejan abiertos y bloqueados por error. Cuando esto sucede, es imposible tener acceso a las partes bloqueadas de un archivo desde otros equipos de la red. Use la opción */close* del comando *net file* para quitar el bloqueo y cerrar el archivo.

Net Group

Agrega, muestra o modifica grupos globales en dominios de Windows NT Server. Este comando sólo está disponible en los dominios de Windows NT Server.

net group [nombre_grupo [/comment:"texto"]] [/domain]

net group nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]

net group nombre_grupo nombre_usuario[...] {/add | /delete} [/domain]

Parámetros

Ninguno

Escriba *net group* sin parámetros para mostrar el nombre de un servidor y los nombres de los grupos de dicho servidor.

Nombre_grupo

Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Especifique un nombre de grupo para ver la lista de los usuarios correspondientes.

/comment:"texto"

Agrega un comentario para un grupo nuevo o existente. Dicho comentario puede tener hasta 48 caracteres. Escriba el texto entre comillas.

/domain

Realiza la operación sobre el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local.

Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De manera predeterminada, los equipos con Windows NT Server realizan

las operaciones en el controlador principal del dominio.

Nombre_usuario[...]

Muestra la lista de uno o más usuarios que se agregarán o quitarán de un grupo. Separe los nombres de usuario con un espacio en blanco.

/add

Agrega un grupo o un nombre de usuario a un grupo. Debe establecerse una cuenta para los usuarios agregados a un grupo con este comando.

/delete

Quita un grupo o un nombre de usuario de un grupo.

Ejemplos

Para ver una lista de todos los grupos en el servidor local, escriba:

net group

Para agregar un grupo llamado ejec a la base de datos local de cuentas de usuario, escriba:

net group ejec /add

Para agregar un grupo llamado ejec a la base de datos de cuentas de usuario de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado, escriba:

net group ejec /add /domain

Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec en el equipo local, escriba:

net group ejec esterv rafar jesust /add

Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado, escriba:

net group ejec esterv rafar jesust /add /domain

Para mostrar los usuarios del grupo ejec, escriba:

net group ejec

Para agregar un comentario al registro del grupo ejec, escriba:

net group ejec /comment:"Plantilla de ejecutivos."

Notas

Este comando puede escribirse también como net groups.

Use el comando net group para agrupar usuarios que trabajan de un modo igual o similar en la red. Cuando se asignen derechos a un grupo, cada miembro recibirá automáticamente estos derechos.

Net Help

Proporciona una lista de comandos de red y temas sobre los que puede obtener ayuda, o proporciona ayuda acerca de un comando o tema específico. Los comandos de red disponibles también se muestran en la ventana Comandos de esta Referencia de comandos, bajo la letra N.

net help [comando]

net comando {/help | /?}

Parámetros

Ninguno

Escriba *net help* sin parámetros para mostrar una lista de comandos y temas acerca de los cuales puede obtenerse ayuda.

Comando

Es el comando acerca del cual desea obtener ayuda. No escriba net como parte del comando.

/help

Proporciona una forma alternativa de mostrar en pantalla el texto de ayuda.

/?

Muestra la sintaxis correcta del comando.

Ejemplos

Para obtener la misma información acerca del comando net use, utilizando dos formas del comando net help, escriba:

net help use

o bien

net use /help

Para ver la sintaxis del comando net use, escriba:

net use /?

Net Helpmsg

Proporciona ayuda referente a un mensaje de error de Windows NT.

net helpmsg mensaje_nº

Parámetros

Mensaje_nº

Es el número de cuatro dígitos del mensaje de Windows NT acerca del cual necesita ayuda.

Notas

Cuando falla una operación de red, se muestra un mensaje similar al siguiente:

NET 2182: El servicio solicitado ya ha sido iniciado.

El comando net helpmsg explica la causa de un error e indica cómo resolver el problema.

Net Localgroup

Agrega, muestra o modifica grupos locales.

net localgroup [nombre_grupo [/comment:"texto"]] [/domain]

net localgroup nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]

net localgroup nombre_grupo nombre [...] {/add | /delete} [/domain]

Parámetros

Ninguno

Escriba *net localgroup* sin parámetros para mostrar el nombre del servidor y los nombres de los grupos locales de dicho equipo.

Nombre_grupo

Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Proporcione sólo un nombre_grupo para ver una lista de los usuarios o grupos globales de un grupo local.

/comment:"texto"

Agrega un comentario para un grupo nuevo o existente. El comentario puede tener hasta 48 caracteres de longitud. Escriba el texto deseado entre comillas.

/domain

Realiza la operación en el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local.

Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. Si no se indica lo contrario, los equipos con Windows NT Server realizarán las operaciones en el controlador principal del dominio.

nombre [...]

Muestra la lista de uno o más nombres de usuario o de grupo que se agregarán a un grupo local o se quitarán de él. Separe cada nombre con un espacio en blanco. Los nombres pueden ser usuarios locales, usuarios de otros dominios o grupos globales, pero no otros grupos locales. Si un usuario es de otro dominio, escriba el nombre de usuario después del nombre de dominio (por ejemplo, VENTAS\SAMUEL).

/add

Agrega un nombre de grupo o de usuario a un grupo local. Debe establecerse una cuenta para los usuarios o grupos globales que se agreguen a un grupo local con este comando.

/delete

Quita un nombre de grupo o de usuario de un grupo local.

Use el comando net localgroup para agrupar usuarios que utilizan de un modo igual o similar el equipo o la red. Cuando se asignen derechos a un grupo local, cada miembro de dicho grupo recibirá automáticamente estos derechos.

Ejemplos

Para mostrar una lista de todos los grupos locales del servidor local, escriba:

net localgroup

Para agregar un grupo local llamado ejec a la base de datos local de cuentas de usuario, escriba:

net localgroup ejec /add

Para agregar un grupo local llamado ejec a la base de datos de cuentas de usuario de un dominio de Windows NT Server, escriba:

net localgroup ejec /add /domain

Para agregar las cuentas de usuario ya existentes esterv, rafar (del dominio VENTAS) y jesust al grupo local ejec en el equipo local, escriba:

net localgroup ejec esterv ventas\rafar jesust /add

Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de Windows NT Server, escriba:

net localgroup ejec esterv rafar jesust /add /domain

Para mostrar los usuarios del grupo local ejec, escriba:

net localgroup ejec

Para agregar un comentario al registro del grupo local ejec, escriba:

net localgroup ejec /comment:"Plantilla de ejecutivos."

Net Name

Agrega o elimina un nombre para mensajes (a veces llamado alias), o muestra la lista de nombres para los que el equipo aceptará mensajes. Para poder usar net name, el servicio de Mensajería debe estar en ejecución.

net name [nombre [/add | /delete]]

Parámetros

Ninguno

Escriba *net name* sin parámetros para mostrar una lista de los nombres actualmente en uso.

Nombre

Especifica el nombre que recibe mensajes. Dicho nombre puede tener un máximo de 15 caracteres.

/add

Agrega un nombre a un equipo. Escribir /add es opcional puesto que el resultado de escribir net name nombre es el mismo que el de escribir net name nombre /add.

/delete

Quita un nombre de un equipo.

Ejemplos

Para ver la lista de nombres en su equipo, escriba:

net name

Para agregar el nombre rsvp a su equipo, escriba:

net name rsvp

Para quitar el nombre rsvp de su equipo, escriba:

net name rsvp /delete

Notas

Use el comando net name para especificar un nombre para la recepción de mensajes. Para poder usar este comando, debe haberse iniciado el servicio Mensajería. Cada nombre de mensajería debe ser único en la red. Los nombres creados con net name se destinan estrictamente a mensajes; estos nombres no son grupos.

Windows NT usa tres tipos de nombres:

Cualquier nombre para mensajería, que se agrega con net name.

El nombre de equipo del equipo, que se agrega al iniciar el servicio Estación de trabajo.

Su nombre de usuario, que se agrega cuando inicia la sesión, suponiendo que su nombre no se esté usando como nombre de mensajería en otra parte de la red.

Net Pause

Interrumpe los servicios en ejecución.

net pause servicio

Parámetros

Servicio

Puede ser:

Servidor de archivos para Macintosh (sólo en Windows NT Server).

Servicio de publicación de FTP.

LPDSVC.

Inicio de sesión de red.

DDE de red.

DSDM DDE de red.

Proveedor de seguridad Lan Manager de NT.

Inicio remoto (sólo en Windows NT Server).

Servidor de acceso remoto.

Schedule.

Servidor.

Servicios simples de TCP/IP.

Estación de trabajo.

Ejemplos

Para interrumpir el servicio Servidor, escriba:

net pause server

Para interrumpir el servicio Inicio de sesión de red, escriba:

net pause "net logon"

Notas

En un servidor:

Use el comando net pause antes de detener un servicio para permitir que los usuarios finalicen su trabajo o se desconecten de los recursos. Hacer una pausa en un servicio lo interrumpe momentáneamente, pero no elimina el software de la memoria. Los usuarios que están conectados a un recurso pueden finalizar sus tareas, pero no podrán efectuar nuevas conexiones a dicho recurso.

Si piensa detener un servicio que afecta a recursos compartidos, primero interrúmpalo, luego envíe un mensaje con el comando net send para avisar de dicha detención; después de un lapso suficiente para que los usuarios terminen de usar el servicio, deténgalo usando el comando net stop.

Para volver a activar un servicio interrumpido, use el comando net continue.

En un cliente:

Use los comandos net pause y net continue para pasar de las impresoras de la red a las impresoras conectadas a su estación de trabajo.

Tanto en un servidor como en un cliente:

No se pueden interrumpir todos los servicios.

La pausa afecta a los servicios de Windows NT de las siguientes formas:

La pausa del servicio Inicio de sesión de red impide que el equipo procese las peticiones de inicio de sesión. Si el dominio tiene otros servidores de inicio de sesión, los usuarios podrán iniciar su sesión en la red.

La pausa del servicio Servidor impide que los usuarios establezcan nuevas conexiones con los recursos compartidos de éste y, si no hay otros servidores de inicio de sesión en la red, impide que los usuarios inicien su sesión en la red. Esto no afecta a una conexión existente. Los administradores pueden establecer conexiones con el servidor aunque el servicio esté interrumpido.

La pausa del servicio Estación de trabajo mantiene el nombre de usuario, la contraseña y las conexiones definidas, pero dirige las peticiones de impresión a las impresoras conectadas al equipo, en lugar de hacerlo a las impresoras conectadas a la red.

Net Print

Muestra o controla los trabajos y las colas de impresión.

net print \\nombre_equipo\recurso_compartido

net print [\\nombre_equipo] trabajo_nº [/hold | /release | /delete]

Parámetros

Nombre_equipo

Es el nombre del equipo que comparte las colas de impresión.

Recurso_compartido

Es el nombre de la cola de impresión. Cuando incluya recurso_compartido y nombre_equipo, sepárelos con una barra invertida (\).

Trabajo_nº

Es el número de identificación asignado a un trabajo de impresión en una cola. Un equipo con una o más colas de impresión asigna a cada trabajo un número único. Si se está usando un número de trabajo en una cola compartida por un equipo, dicho número no se asignará a ningún otro trabajo, ni siquiera a otras colas de ese equipo.

/hold

Cuando se usa con trabajo_nº, retiene el trabajo en espera en la cola de impresión. El trabajo permanece en la cola y los demás trabajos lo rebasarán hasta que se libere.

/release

Libera un trabajo o una cola de impresión que se ha retenida.

/delete

Quita un trabajo de la cola de impresión.

Ejemplos

Para obtener información acerca del trabajo número 35 del equipo \\PRODUCCIÓN, escriba:

net print \\producción 35

Para retener el trabajo número 263 del equipo \\PRODUCCIÓN, escriba:

net print \\producción 263 /hold

Para liberar el trabajo número 263 del equipo \\PRODUCCIÓN, escriba:

net print \\producción 263 /release

Para obtener una lista del contenido de la cola de impresión MATRIZ del equipo \\PRODUCCIÓN, escriba:

net print \\producción\matriz

Notas

El comando net print muestra información en distintos formatos acerca de las colas de impresión.

Puede hacer que se presente una cola en particular usando:

net print \\nombre_equipo\recurso_compartido.

Net Send

Envía mensajes a otros usuarios, equipos, grupos o nombres para mensajes en la red. El servicio Mensajería debe estar en ejecución para poder recibir mensajes.

*net send {nombre | * | /domain[:nombre] | /users} mensaje*

Parámetros

Nombre

Es el nombre de usuario, de equipo o nombre para mensajes al que se envía el mensaje. Si se trata de un nombre de equipo que contiene caracteres en blanco, escríbalo entre comillas (" ").

*

Envía el mensaje a todos los nombres del grupo.

/domain[:nombre]

Envía el mensaje a todos los nombres del dominio del equipo. Si se especifica nombre, se enviará el mensaje a todos los nombres del dominio o grupo de trabajo especificado.

/users

Envía el mensaje a todos los usuarios conectados al servidor.

Mensaje

Es el texto que se enviará como mensaje.

Ejemplos

Para enviar el mensaje "Reunión cambiada a las 15 horas. En el mismo lugar." al usuario robertof, escriba:

net send robertof Reunión cambiada a las 15 horas. En el mismo lugar.

Para enviar un mensaje a todos los usuarios conectados al servidor, escriba:

net send /users Este servidor se apagará en 5 minutos.

Para enviar un mensaje que incluya una barra diagonal, escriba:

net send robertof "Formatear tu disco con FORMAT /4"

Notas

Sólo puede enviar un mensaje a un nombre que esté activo en la red. Si lo envía a un nombre de usuario, éste debe haber iniciado una sesión y estar ejecutando el servicio Mensajería para recibir el mensaje.

Enviar mensajes a varios usuarios

Windows NT proporciona varios métodos para transmitir mensajes. Puede hacerlo a todos los nombres del dominio de su equipo (con * o /domain) o a otro dominio diferente (/domain:nombre). Los mensajes transmitidos pueden tener hasta 128 caracteres.

La opción /users permite enviar un mensaje a todos los usuarios que tienen sesiones en el servidor. Los parámetros que envían mensajes a varios usuarios deben usarse con precaución.

Net Session

Muestra la lista o desconecta las sesiones entre un equipo local y los clientes conectados a él.

net session [\\nombre_equipo] [/delete]

Parámetros

Ninguno

Escriba net session sin parámetros para que se muestre información acerca de todas las sesiones con el equipo local.

\ \ Nombre_equipo

Identifica el equipo para el cual se mostrarán o desconectarán sesiones.

/delete

Finaliza la sesión del equipo con \\nombre_equipo y cierra todos los archivos abiertos en el equipo para la sesión. Si se omite \\nombre_equipo, se cancelarán todas las sesiones del equipo local.

Ejemplos

Para mostrar una lista con información sobre las sesiones del servidor local, escriba:

net session

Para mostrar información sobre las sesiones del cliente cuyo nombre de equipo es SÁNCHEZ, escriba:

net session \\sánchez

Para finalizar todas las sesiones entre el servidor y los clientes conectados, escriba:

net session /delete

Notas

El comando *net session* puede escribirse también como *net sessions* o *net sess*.

Use el comando *net session* para ver en pantalla los nombres de equipo y nombres de usuario de aquellos usuarios que tienen acceso a un servidor, si tienen archivos abiertos y cuánto tiempo ha permanecido inactiva la sesión de cada uno de ellos.

Una sesión queda registrada cuando un usuario de un cliente entra en contacto con un servidor. Esto ocurre cuando los dos sistemas están en la misma red y el servidor acepta el nombre y la contraseña del usuario. Un usuario de un cliente debe tener una sesión iniciada en el servidor antes de poder usar los recursos compartidos del mismo; una sesión no se establece hasta que el usuario de un cliente se conecta a un recurso. Entre un cliente y un servidor sólo puede existir una sesión, pero puede haber varios puntos de entrada, o conexiones, a los recursos.

Para determinar el tiempo que puede permanecer inactiva una sesión antes de que se desconecte

automáticamente, active la característica autodisconnect con la opción /autodisconnect del comando net config server. El usuario no interviene en este tipo de desconexión, puesto que Windows NT reanuda automáticamente la conexión en cuanto el usuario vuelve a usar el recurso.

Para finalizar una sesión con el servidor, use la opción /delete junto con \\nombre_equipo.

Net Share

Crea, elimina o muestra recursos compartidos.

net share recurso_compartido

net share recurso_compartido [/users:número | unlimited] [/remark:"texto"]

net share {recurso_compartido | unidad:ruta_de_acceso} /delete

Parámetros

Ninguno

Escriba net share sin parámetros para mostrar información acerca de todos los recursos compartidos en el equipo local.

Recurso_compartido

Es el nombre de red del recurso compartido. Escriba net share con un recurso_compartido únicamente para mostrar información acerca de dicho recurso compartido.

Unidad:ruta_de_acceso

Especifica la ruta de acceso absoluta del directorio que va a compartirse.

/users:número

Establece el número máximo de usuarios que pueden tener acceso simultáneamente al recurso compartido.

/unlimited

Especifica que puede tener acceso simultáneamente al recurso compartido un número ilimitado de usuarios.

/remark:"texto"

Agrega un comentario descriptivo acerca del recurso. Escriba el texto entre comillas.

/delete

Deja de compartir un recurso.

Ejemplos

Para mostrar información acerca de los recursos compartidos en el equipo, escriba:

net share

Para compartir el directorio C:\CARTAS de un equipo con el nombre compartido SECRETARIA e incluir un comentario, escriba:

net share secretaria=c:\cartas /remark:"Para el departamento 123."

Para dejar de compartir el directorio CARTAS, escriba:

net share secretaria /delete

Para compartir el directorio C:\LST FIG de un equipo con el nombre compartido LISTA, escriba:

net share lista="c:\lst fig"

Notas

Use el comando *net share* para compartir recursos.

Para compartir un directorio con una ruta de acceso que contiene un carácter en blanco, escriba la unidad y la ruta del directorio entre comillas (" ").

Cuando se muestran todos los recursos compartidos de un equipo, Windows NT indica el nombre del recurso compartido, el nombre o nombres de dispositivo o rutas de acceso asociadas con el recurso y un comentario descriptivo acerca de éste.

Los recursos compartidos de un servidor se guardan a medida que se crean. Cuando detenga el servicio Servidor, todos los recursos compartidos se desconectarán, pero se volverán a conectar automáticamente en cuanto vuelva a iniciarse el servicio o cuando se reinicie el equipo.

Net Start

Inicia un servicio o muestra una lista de los servicios iniciados. Los nombres de servicios que son de dos o más palabras, como Inicio de sesión de red o Examinador de equipos, deben estar entre comillas (").

net start [servicio]

Parámetros

Ninguno

Escriba *net start* sin parámetros para mostrar una lista de los servicios en ejecución.

Servicio

Puede ser:

Alerta

Servicio de cliente para netware

Servidor del Portafolio

Examinador de equipos

Cliente dhcp

Duplicador de directorios

Registro de sucesos

Servicio de publicación de FTP

LPDSVC

Mensajería

Inicio de sesión de red

DDE de red

DSDM DDE de red

Agente de supervisión de red

Proveedor de seguridad nt lm

OLE

Administrador de conexiones de acceso remoto

Servicio isnsap de acceso remoto

Servidor de acceso remoto

Localizador de llamada a procedimientos remotos (rpc)

Servicio de llamada a procedimientos remotos (rpc)

Schedule

Servidor

Servicios simples de tcp/ip

SNMP

Spooler

Ayuda de netbios de tcp/ip

SAI

Estación de trabajo

Los siguientes servicios sólo están disponibles en Windows NT Server:

Servidor de archivos para Macintosh

Servicio de puerta de enlace o gateway para netware

Servidor de DHCP de Microsoft

Servidor de impresión para Macintosh

Inicio remoto

Servicio de nombres Internet de Windows

Notas

Use el comando *net start* servicio para iniciar un servicio de Windows NT. Algunos servicios dependen de otros servicios.

Puede utilizar la opción Servicios en el Panel de control para configurar el inicio y la detención automática de los servicios. Esta opción también le permite detener, iniciar, interrumpir y continuar los servicios de red manualmente.

Los nombres de servicios que constan de dos o más palabras, como Inicio de sesión de red o Examinador de equipos, deben estar entre comillas (").

Este comando también inicia los servicios de red que no están incluidos en Windows NT.

Los servicios que pueden iniciarse son:

Net Start "Administrador de conexiones de acceso remoto"

Net Start "Agente de supervisión de red"

Net Start "Ayuda de NetBIOS de TCP/IP"

Net Start "Cliente de DHCP"

Net Start "DDE de red"

Net Start "Duplicador de directorios"

Net Start "Estación de trabajo"

Net Start "Examinador de equipos"

Net Start "Inicio de sesión de red"

Net Start "Inicio remoto"

Net Start "Localizador de rpc"

Net Start "Proveedor de seguridad NT LM"

Net Start "Registro de sucesos"

Net Start "Servicio de cliente para NetWare"

Net Start "Servicio de llamada a procedimientos remotos (RPC)"

Net Start "Servicio de nombres Internet de Windows"

Net Start "Servicio de publicación de FTP"

Net Start "Servicio de puerta de enlace o gateway para NetWare"

Net Start "Servicio ISNSAP de acceso remoto"

Net Start "Servicio Schedule"

Net Start "Servicios simples de TCP/IP"

Net Start "Servidor de acceso remoto"

Net Start "Servidor de archivos para Macintosh"

Net Start "Servidor de dde de red"

Net Start "Servidor de impresión para Macintosh"

Net Start "Servidor de Portafolio"

Net Start "Servidor DHCP de Microsoft"

Net Start Alerta

Net Start Lpdsvc

Net Start Mensajería

Net Start Sai

Net Start Servidor

Net Start Snmp

Net Start Spooler

Net Statistics

Muestra el registro de estadísticas del servicio local Estación de trabajo o Servidor.

net statistics [workstation | server]

Parámetros

Ninguno

Escriba *net statistics* sin parámetros para obtener una lista de los servicios en ejecución para los cuales hay datos estadísticos disponibles.

Workstation

Muestra los datos estadísticos del servicio local Estación de trabajo.

Server

Muestra los datos estadísticos del servicio local Servidor.

Ejemplos

Para mostrar los servicios en ejecución para los que hay estadísticas disponibles, escriba:

net stats

Para mostrar las estadísticas del servicio Servidor y evitar que se desplace la pantalla, escriba:

net statistics server | more

Notas

Este comando puede escribirse también como net stats.

Use el comando *net statistics* para mostrar información sobre el rendimiento del servicio especificado.

El servicio Servidor:

Windows NT indica el nombre de equipo del equipo, la fecha y hora en que se actualizaron por última vez las estadísticas, y proporciona la siguiente información:

El número de sesiones que se iniciaron, se desconectaron automáticamente y se desconectaron a causa de un error.

El número de kilobytes enviados y recibidos, y el tiempo medio de respuesta del servidor.

El número de errores e infracciones de contraseña y límites de permiso.

El número de veces que se usaron los archivos, impresoras y dispositivos de comunicaciones compartidos.

El número de veces que se excedió el tamaño del búfer de memoria.

El servicio Estación de trabajo:

Windows NT indica el nombre de equipo del equipo, la fecha y hora en que se actualizaron por última vez las estadísticas, y proporciona la siguiente información:

El número de bytes y SMB recibidos y transmitidos.

El número de operaciones de lectura y escritura logradas o fallidas.

El número de errores de la red.

El número de sesiones fallidas, desconectadas o conectadas nuevamente.

El número de conexiones a recursos compartidos logradas o fallidas.

Net Stop

Detiene un servicio de Windows NT.

net stop servicio

Parámetros

Servicio

Puede ser alerta, servicio de cliente para netware, servidor del Portafolio, examinador de equipos, duplicador de directorios, servicio de publicación de FTP, lpdsvc, mensajería, inicio de sesión de red, dde de red, dsdm dde de red, agente de supervisión de red, proveedor de seguridad nt lm, ole, administrador de conexiones de acceso remoto, servicio isnsap de acceso remoto, servidor de acceso remoto, localizador de llamada a procedimientos remotos (rpc), schedule, servidor, servicios simples de tcp/ip, snmp, spooler, ayuda de netbios de tcp/ip, sai y estación de trabajo.

Los siguientes servicios sólo están disponibles en Windows NT Server:

Servidor de archivos para macintosh.

Servicio de puerta de enlace o gateway para netware.

Servidor dhcp de microsoft.

Servidor de impresión para macintosh.

Servicio de nombres internet de windows.

Notas

Detiene un servicio para suprimir la función que realiza en la red y para eliminar el software de la memoria.

Al detener el servicio Servidor se impide que los usuarios tengan acceso a los recursos compartidos del equipo. Si detiene el servicio Servidor cuando los usuarios están teniendo acceso a los recursos, Windows NT mostrará un mensaje de advertencia pidiendo confirmación antes de cancelar las conexiones. Una respuesta afirmativa cancelará todas las conexiones con el equipo.

Antes de detener el servicio Servidor, puede hacer lo siguiente:

Efectuar una pausa en el servicio (para no permitir nuevas conexiones).

Enviar un mensaje advirtiendo a los usuarios de que deben desconectarse de los recursos del servidor.

Net stop también puede detener servicios de red no suministrados con Windows NT.

Net Time

Sincroniza el reloj del equipo con el de otro equipo o dominio. Si se utiliza sin la opción /set, muestra la hora de otro equipo o dominio.

net time [\\nombre_equipo | /domain[:nombre]] [/set]

Parámetros

\\ Nombre_equipo

Es el nombre del servidor que desee comprobar o con el que desee sincronizar las estaciones de trabajo.

/domain[:nombre]

Es el dominio con el que desea sincronizar la hora.

/set

Sincroniza el reloj del equipo con el del equipo o dominio especificado.

Net Use

Conecta o desconecta un equipo de un recurso compartido o muestra información acerca de las conexiones del equipo. También controla las conexiones de red persistentes.

*net use [nombre_dispositivo] [\\nombre_equipo\recurso_compartido[\volumen]] [contraseña | *]] [/user:[nombre_dominio\]nombre_usuario] [[/delete] | [/persistent:{yes | no}]]*

*net use nombre_dispositivo [/home[contraseña | *]] [/delete:{yes | no}]*

net use [/persistent:{yes | no}]

Parámetros

Ninguno

Escriba net use sin parámetros para obtener una lista de las conexiones de red.

Nombre_dispositivo

Asigna un nombre para la conexión al recurso o especifica el dispositivo que se va a desconectar. Hay dos tipos de nombres de dispositivos: unidades de disco (D a Z) e impresoras (LPT1 a LPT3). Escriba un asterisco en lugar de un nombre específico de dispositivo para asignar el siguiente nombre de dispositivo disponible.

\\nombre_equipo\recurso_compartido

Es el nombre del servidor y del recurso compartido. Si el nombre de equipo contiene caracteres en blanco,

escriba la barra invertida doble (\\) y el nombre entre comillas(" "). El nombre de equipo puede tener entre 1 y 15 caracteres.

\volumen

Especifica un volumen NetWare del servidor. Para poder conectarse con servidores NetWare debe tener instalado y estar ejecutando el Servicio de cliente para NetWare (Windows NT Workstation) o el Servicio de puerta de enlace o gateway para NetWare (Windows NT Server).

Contraseña

Es la contraseña necesaria para tener acceso al recurso compartido.

*

Pide por la contraseña. Los caracteres no se muestran en pantalla a medida que los escribe.

/user

Especifica un nombre de usuario diferente con el que se realiza la conexión.

nombre_dominio

Especifica otro dominio. Por ejemplo, net use d: \\servidor\recurso_compartido /user:admin\mario conecta el usuario mario de la misma forma que si la conexión se realizara desde el dominio administrador. Si se omite el dominio, se usará aquél en el que tenga lugar la conexión actual.

Nombre_usuario

Especifica el nombre de usuario con el que se iniciará la sesión.

/home

Conecta un usuario con su directorio particular.

/delete

Cancela la conexión de red especificada. Si el usuario especifica la conexión mediante un asterisco se cancelarán todas las conexiones de red.

/persistent

Controla el uso de conexiones de red persistentes. El valor predeterminado es la última configuración utilizada. Las conexiones sin dispositivos no son persistentes.

Yes

Guarda todas las conexiones tal como se realizaron y las restaura en el siguiente inicio de sesión.

No

No guarda la conexión en curso ni las siguientes. Las existentes se restaurarán en el siguiente inicio de sesión.

Use el modificador /delete para eliminar conexiones persistentes.

Ejemplos

Para asignar el nombre de dispositivo de unidad de disco E: al directorio compartido CARTAS del servidor \\FINANCIERO, escriba:

net use e: \\financiero\cartas

Para asignar el nombre de dispositivo de unidad de disco M: al directorio MARÍA dentro del volumen CARTAS del servidor NetWare FINANCIERO, escriba

net use m: \\financiero\cartas\maría

Para asignar el nombre de dispositivo LPT1 a la cola de la impresora compartida LÁSER2 del servidor \\CONTABILIDAD, escriba:

net use lpt1: \\contabilidad\láser2

Para desconectarse de la cola de impresora LPT1, escriba:

net use lpt1: /delete

Para asignar el nombre de dispositivo de unidad de disco H: al directorio particular del usuario mario, escriba:

net use h: \\contabilidad\usuarios /home /user:mario

Para asignar el nombre de dispositivo de unidad de disco F: al directorio compartido NOTAS del servidor \\FINANCIERO, que requiere la contraseña hctarcs, sin que la conexión sea persistente, escriba:

net use f: \\financiero\notas hctarcs /persistent:no

Para desconectarse del directorio \\FINANCIERO\NOTAS, escriba:

net use f: \\financiero\notas /delete

Para conectarse a un recurso compartido del servidor FINANCIERO2, escriba:

net use k: "\\financiero 2"\circulares

Si el nombre del servidor incluye un espacio en blanco, escríbalo entre comillas; de lo contrario, Windows NT mostrará un mensaje de error.

Para restaurar las conexiones actuales cada vez que se inicie una sesión, independientemente de cambios futuros, escriba:

net use /persistent:yes

Notas

Utilice el comando net use para efectuar la conexión o desconexión de un recurso de la red y para ver sus conexiones actuales con dichos recursos. Es imposible desconectarse de un directorio compartido si se utiliza

como unidad actual o si está en uso por un proceso activo.

Hay varias formas de obtener información acerca de una conexión:

Escriba net use nombre_dispositivo para obtener información acerca de una conexión específica.

Escriba net use para obtener una lista de todas las conexiones del equipo.

Conexiones sin dispositivos

Las conexiones sin dispositivos no son persistentes.

Conexión con servidores NetWare

Una vez que el software Servicio de cliente para NetWare o Servicio de puerta de enlace o gateway para NetWare está instalado y en ejecución, podrá conectarse a un servidor NetWare en una red Novell. Utilice la misma sintaxis que al conectarse a un servidor de red de Windows, excepto que debe incluir el volumen con el que desea conectarse.

Net User

Agrega o modifica cuentas de usuario o muestra información acerca de ellas.

*net user [nombre_usuario [contraseña | *] [opciones]] [/domain]*

*net user nombre_usuario {contraseña | *} /add [opciones] [/domain]*

net user nombre_usuario [/delete] [/domain]

Parámetros

Ninguno

Escriba *net user* sin parámetros para ver una lista de las cuentas de usuario del equipo.

nombre_usuario

Es el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o ver. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

Contraseña

Asigna o cambia una contraseña para la cuenta de usuario. Una contraseña debe tener la longitud mínima establecida con la opción /minpwlen del comando net accounts y puede tener un máximo de 14 caracteres.

*

Pide la contraseña. Los caracteres no se muestran en pantalla a medida que los escribe.

/domain

Realiza la operación en el controlador principal del dominio principal del equipo.

Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. De forma predeterminada, los equipos con Windows NT Server realizan las operaciones en el controlador principal de dominio.

NOTA: Esta acción se lleva a cabo en el controlador principal del dominio principal del equipo. Puede que no se inicie la sesión en el dominio.

/add

Agrega una cuenta de usuario a la base de datos de cuentas de usuario.

/delete

Quita una cuenta de usuario de la base de datos de cuentas de usuario.

Opciones

/active:{no | yes}

Desactiva o activa la cuenta de usuario. Si no está activa, el usuario no puede tener acceso a los recursos del equipo. El valor predeterminado es yes (activa).

/comment:"texto"

Proporciona un comentario descriptivo acerca de la cuenta de usuario. Puede tener hasta 48 caracteres. Escriba el texto entre comillas.

/countrycode:nnn

Usa los códigos de país del sistema operativo para instalar los archivos de ayuda y mensajes de error en el idioma especificado. Un valor 0 significa el código de país predeterminado.

/expires:{fecha | never}

El parámetro fecha establece una fecha de caducidad de la cuenta de usuario, mientras que never determina una duración ilimitada de dicha cuenta. Las fechas de caducidad pueden darse en el formato mm/dd/aa, dd/mm/aa o mm,dd,aa, dependiendo de /countrycode. Observe que la cuenta caduca al comienzo de la fecha especificada. Los meses pueden indicarse con un número, con todas sus letras o abreviados con tres letras. Los años pueden constar de dos o cuatro dígitos. Utilice comas o barras diagonales para separar las partes de la fecha (no espacios en blanco). Si se omite aa, se asume el año de la siguiente fecha (de acuerdo con la fecha y hora de su equipo). Por ejemplo, las siguientes entradas de fecha son equivalentes si se introducen entre el 10 de enero de 1994 y el 8 de enero de 1995.

jan,9 /9/95 ,9,1995 /9

/fullname:"nombre"

Agrega un determinado nombre al usuario en lugar de su nombre de usuario normal. Escriba dicho nombre entre comillas.

/homedir:ruta_acceso

Establece la ruta de acceso del directorio particular del usuario. Dicha ruta debe ser una ya existente.

/homedirreq:{yes | no}

Establece si es necesario un directorio particular.

/passwordchg:{yes | no}

Especifica si los usuarios pueden cambiar su contraseña. El valor predeterminado es yes.

/passwordreq:{yes | no}

Especifica si una cuenta de usuario debe tener una contraseña. El valor predeterminado es yes.

/profilepath[:ruta_acceso]

Establece una ruta de acceso para el perfil de inicio de sesión del usuario. Dicha ruta lleva a un perfil de registro.

/scriptpath:ruta_acceso

Establece una ruta de acceso al archivo de comandos de inicio de sesión del usuario. Ruta_acceso no puede ser una ruta absoluta; es relativa a %raíz_sistema%\SYSTEM32\REPL\IMPORT\SCRIPTS.

/times:{horas | all}

Especifica las horas en las que se permite al usuario el uso del equipo. El valor horas se expresa como día

[−día][,día[−día]] ,hora[−hora][,hora[−hora]], limitado a incrementos de una hora. Los días se pueden deletrear o abreviar (L,M,Mi,J,V,S,D). Las horas se pueden escribir en formato de 12 ó 24 horas. Para el formato de 12 horas, use AM, PM, o A.M., P.M. El valor all significa que un usuario puede iniciar una sesión en cualquier momento. Un valor nulo (en blanco) significa que un usuario nunca puede iniciar la sesión. Separe el día y la hora mediante comas, y las unidades de día y hora con punto y coma (por ejemplo, L,4AM−5PM;M,1AM−3PM). No use espacios en la especificación de /times.

/usercomment:"texto"

Permite que un administrador agregue o cambie el "Comentario de usuario" de la cuenta. Escriba el texto entre comillas.

/workstations:{nombre_equipo [,...] | *}

Lista de hasta ocho estaciones de trabajo desde las que un usuario puede iniciar una sesión en la red. Separe los nombres de las estaciones con una coma. Si /workstation no es una lista o ésta es igual a un *, el usuario puede iniciar una sesión desde cualquier equipo.

Ejemplos

Para mostrar una lista de todas las cuentas de usuario del equipo local, escriba:

net user

Para ver información acerca de la cuenta juanh, escriba:

net user juanh

Para agregar una cuenta de usuario para Enrique Pérez, con derechos de inicio de sesión desde las 8 A.M. a 5 P.M. de lunes a viernes (sin espacios en las especificaciones de las horas), una contraseña obligatoria y el nombre completo del usuario, escriba:

net user enriquep enriquep /add /passwordreq:yes /times:lunes−viernes,8am−5pm/fullname:"Enrique Pérez"

El nombre de usuario (enriquep) se escribe la segunda vez como contraseña.

Para establecer la hora de inicio de sesión de juansp (8 A.M. a 5 P.M.) usando la notación de 24 horas, escriba:

net user juansp /time:Lun−Vie,08:00−17:00

Para establecer la hora de inicio de sesión de juansp (8 A.M. a 5 P.M.) usando la notación de 12 horas, escriba:

net user juansp /time:Lun−Vie,8am−5pm

Para especificar las horas de inicio de sesión de 4 A.M. a 5 P.M. los Lunes, 1 P.M. a 3 P.M. los Martes, y 8 A.M. a 5 P.M. de Miércoles a Viernes para maríasl, escriba:

net user maríasl /time:Lun,4am−5pm;Mar,1pm−3pm;Mie−Vie,8:00−17:00

Para establecer /homedirreq en yes para enriquep y asignarle \\SERVIDOR\USUARIOS\\ENRIQUEP como directorio particular, escriba:

net user enriquep /homedirreq:yes

/homedir \\SERVIDOR\USUARIOS\ENRIQUEP

Notas

Este comando puede escribirse también como net users.

Use el comando net user para crear y controlar las cuentas de usuarios de un dominio. La información sobre dichas cuentas se almacena en la base de datos de cuentas de usuario.

Cuando escriba el comando net user en un equipo que ejecute Windows NT Server, los cambios en la base de datos de cuentas se producirán automáticamente en el controlador principal de dominio y luego se duplicarán en los controladores de reserva. Esto es válido únicamente para los dominios de Windows NT Server.

Net View

Muestra una lista de dominios, una lista de equipos o los recursos compartidos en el equipo especificado.

net view [\\nombre_equipo | /domain[:nombre_dominio]]

net view /network:nw [\\nombre_equipo]

Parámetros

Ninguno

Escriba *net view* sin parámetros para mostrar la lista de los equipos del dominio actual.

Nombre_equipo

Especifica el equipo cuyos recursos compartidos desea ver.

/domain[:nombre_dominio]

Especifica el dominio del que se desean ver los equipos disponibles. Si se omite nombre_dominio, se mostrarán todos los dominios de la red.

/network:nw

Muestra todos los servidores disponibles de una red NetWare. Si se especifica un nombre de equipo, se mostrarán los recursos disponibles en dicho equipo de la red NetWare. Mediante esta opción también pueden especificarse otras redes que se hayan agregado al sistema.

Ejemplos

Para ver una lista de los recursos compartidos por el equipo \\PRODUCTOS, escriba:

net view \\productos

Para ver los recursos disponibles en el servidor NetWare \\MARKETING, escriba

net view /network:nw \\marketing

Para ver una lista de los equipos del dominio o grupo de trabajo Ventas, escriba:

net view /domain:ventas

APENDICE1: EJEMPLO PRÁCTICO

Nos han encargado un proyecto que consiste en la informatización de una empresa, en concreto de una empresa de seguros médicos (MEDIBROK).

Esta empresa es de ámbito local, y por el momento sólo dispone de una oficina, aunque ha dejado bien claro que esperan poder ampliar en poco tiempo este número de oficinas y posteriormente tienen planificado el montar oficinas en la península.

Dentro de esta oficina quieren contar con un servidor central, que no sea excesivamente difícil de manejar (es decir no quieren invertir mucho tiempo en enseñar a sus técnicos actuales ni contratar otros nuevos), y unos 25 puestos de trabajo conectados al servidor.

Tiene que haber unas buenas condiciones en lo que a seguridad se refiere, ya que habrá distintos departamentos (el de comerciales, contabilidad, administración y relaciones públicas), y cada uno de los

componentes de estos departamentos en principio no tiene que tener acceso a los datos de los demás departamentos.

También nos han dicho, que desean disponer de un medio para realizar copias de seguridad de la base de datos, donde disponen de la información referente a todos los médicos, asegurados y agentes. (Dicha copia de seguridad no es excesivamente grande). Y de una serie de impresoras (unas tres), para poder imprimir los listados, nóminas y relaciones pertinentes, no necesitando que estos sean a color, pero si de que la impresión sea rápida.

Por otra parte, a ser posible, no querrían cambiar las aplicaciones que poseen, ya que están contentos con ellas y aparte el gasto ascendería ya notablemente.

Con los datos de los que disponemos, la opción a tomar esta clara. Montaremos una red Windows NT. Para ello necesitaremos principalmente:

Un servidor, para lo cual utilizaremos un ordenador con procesador a 450, 256 Mb de RAM (ampliable a 512), con dos discos duros de 6 Gb. A este ordenador le instalaremos como sistema operativo Windows NT Server. A dicho servidor le incorporaremos una unidad de cinta magnética para realizar las copias de seguridad.

Para los puestos de trabajo(25) utilizaremos ordenadores con un procesador a 300, 32 Mb de RAM y un disco duro de 4GB. A estos puestos de trabajo le instalaremos como sistema operativo el Windows NT 4.0 versión Workstation. A tres de estos puestos de trabajo, uno por departamento, se le instalará una impresora láser y se establecerá esta como recurso compartido.

A parte de esto necesitaremos todo el cableado oportuno, así como las tarjetas de red.

Con esto en principio no tendrán ningún tipo problema, y les sobrarán recursos para una administración óptima de la red.

Para dicha gestión podrían dividir la red en dominios maestros únicos o simplemente en grupos de trabajo, esto dependerá del administrador del sistema. Con lo cual el tema de la seguridad quedaría zanjado, y si se quisiera que los miembros de algún dominio accedieran a los recursos de otro (por ejemplo que las chicas de recepción imprimiesen con la impresora que tiene el departamento de administración), simplemente habría que establecer una relación de confianza entre ambos.

BIBLIOGRAFIA

- **Los secretos de Windows NT 4.0,** de Valda Hilley, ediciones ANAYA Multimedia, 1997.
- **El gran libro de Windows NT 4,** MARCOMBO S.A., 1998.
- **Programación avanzada en Windows,** por Jeffrey Richter, McGraw−Hill, 1997.
- **http:// enete.fie.us.es/articulos/...**
- **Revista PC−ACTUAL.**

FTP: Protocolo de transferencia de archivos (File Transport Protocol). Servicio que transfiere archivos ASCII y binarios entre sistemas locales y no locales.

RDSI: Red Digital de Servicios Integrados.

Encaminamiento: Reenvío de paquetes en el camino hasta el destino.

Token Ring: Se basa en al topología de anillo con un método de acceso determinista, en el que la comunicación interna de la red se realiza con la ayuda del procedimiento de testigos (*Tokens)* con una tasa de transferencia 4 o 16 Mbits/s. Sólo la estación que posee el testigo libre puede enviar.

Windows NT 4.0

88