FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

CENTRO DE INFORMACION Y DOCUMENTACION "ING. BRUNO MASCANZONI"

El Centro de Información y Documentación Ing. Bruno Mascanzoni tiene por objetivo satisfacer las necesidades de actualización y proporcionar una adecuada información que permita a los ingenieros, profesores y alumnos estar al tanto del estado actual del conocimiento sobre temas específicos, enfatizando las investigaciones de vanguardia de los campos de la ingeniería, tanto nacionales como extranjeras.

Es por ello que se pone a disposición de los asistentes a los cursos de la DECFI, así como del público en general los siguientes servicios:

* **Préstamo interno.**
* **Préstamo externo.**
* **Préstamo interbibliotecario.**
* **Servicio de fotocopiado.**
* **Consulta a los bancos de datos: librunam, seriunam en cd-rom.**

Los materiales a disposición son:

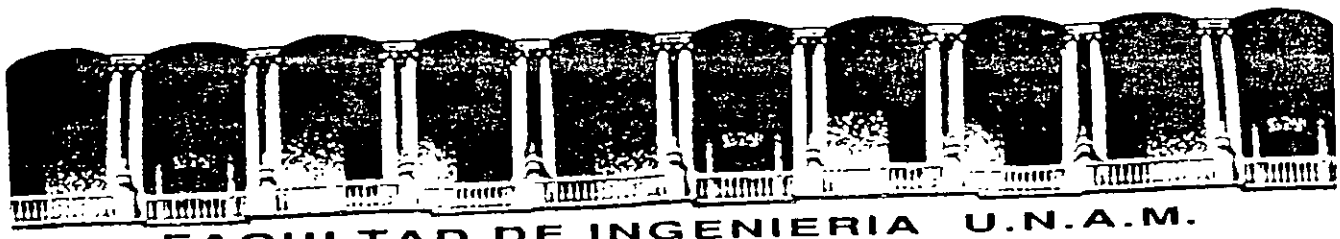
* **Libros.**
* **Tesis de posgrado.**
* **Noticias técnicas.**
* **Publicaciones periódicas.**
* **Publicaciones de la Academia Mexicana de Ingeniería.**
* **Notas de los cursos que se han impartido de 1980 a la fecha.**

En las áreas de ingeniería industrial, civil, electrónica, ciencias de la tierra, computación y, mecánica y eléctrica.

El CID se encuentra ubicado en el mezzanine del Palacio de Minería, lado oriente.

El horario de servicio es de 10:00 a 19:30 horas de lunes a viernes.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26



FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

MODULO III

INSTALACION Y MANEJO DE REDES (LAN)

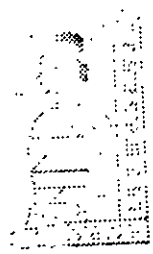
DE MICROS CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

MATERIAL DIDACTICO

OCTUBRE - NOVIEMBRE 1996

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. Tel.: 521-40-20 Apdo. Postal M-2285

INSTALACIÓN Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT



Mayo de 1996

INSTALACION Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT
M O D U L O III (Wnt)

PRESENTACION

Se señaló que en los 80 se inició un movimiento tendencioso hacia las Redes, y que ahora el uso de éstas como herramienta de la computación, es toda una realidad y una necesidad de primer orden.

Es sabido también que los productores del software están luchando por estar a la vanguardia en el mercado internacional, pretendiendo cada firma marcar el "estándar" en las redes, y en este caso MICROSOFT con **WINDOWS NT** como una evolución de su Lan Manager, se está colocando como otro de los sistemas operativos para Redes "a vencer", por ofrecer a los usuarios varias y potentes opciones, por lo que observadores autorizados aseveran que puede llegar a dominar más allá del **mercado corporativo**, ya que ahora es un potente Sistema Operativo de 32 bits, mejora su característica de multitareas y maneja la arquitectura **Cliente-Servidor**.

Tiene a cambio la crítica de la competencia, que sin ser mentira, señala que consume muchos recursos: mínimo un procesador 80386 con 16 MB en RAM y disco duro de buen volumen. Este fenómeno de competencia y continua superación de los productores de software, definitivamente benefician al usuario quien a la postre marca el verdadero **"estándar"**. Conscientes de la evolución y de la necesidad que hay en el medio de las Redes de una actualización profesional **"de punta"**, se ofrece este módulo optativo para el DIPLOMADO, en el que se verá el potencial del producto.

OBJETIVOS

Lograr que los usuarios de **Windows NT y productos de conectividad MICROSOFT** después de este curso, puedan instalar y administrar sus Redes y aplicaciones, aprovechando el potencial y la coyuntura que brinda este software.

Dar otro marco de referencia en cuanto a Sistemas Operativos de Red y mejorar sus conocimientos y manejo en este profundo campo de las Redes.

A QUIEN VA DIRIGIDO

A profesionistas, ejecutivos, y técnicos que por sus necesidades profesionales y aplicaciones estén en la necesidad de conocer **Windows NT y los productos MICROSOFT de conectividad**.

REQUISITOS

Se requiere sin ser limitante, que los participantes tengan conocimientos de los módulos I y II o equivalente, con amplio manejo de MS-DOS y WINDOWS.

INSTALACION Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT
M O D U L O III (Wnt)

T E M A R I O

1.- INTRODUCCIÓN A WINDOWS NT

- Revisión de Conceptos
- Arquitectura Cliente-Servidor
- Interacción de Sistemas Operativos
- Mapas de Memoria
- Componentes del Sistema Operativo de Red
- Características de WINDOWS NT
- " Networking" con WINDOWS NT
- Windows 3.1, 3.11 y Windows 95 en ambiente de Red

2.- INSTALACIÓN DE WINDOWS NT

- Instalación de Hardware
- Instalación de Servidores
- Instalación de Cliente
- Configuración de Sistema Operativo
- Pruebas y diagnostico

3.- GRUPOS DE TRABAJO Y DOMINIOS

- Grupos de Trabajo
- Modelos de Dominio
- Utilerias y administración de dominios

4.- INSTALACION DE ELEMENTOS ESPECIALES

- Puentes, Gatways, UPS
- Discos en espejo, Discos Duplicados
- Cliente acceso remoto
- Otro

5.- EL ADMINISTRADOR Y SUS FUNCIONES

- D o m i n i o s
- Usuarios, Grupos de usuarios, Altas, Bajas
- Atributos y Seguridad
- Manejo de Archivos
- Instalación de aplicaciones
- Impresión con WINDOWS NT
- Monitoreo de la Red
- Corrección de fallas
- Mantenimiento general de la red

6.- SESIONES DE TALLER EN CADA PUNTO DEL TEMARIO

INSTALACIÓN Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

1.- INTRODUCCIÓN A WINDOWS NT

Mayo de 1996.

Introducción a Windows NT Advanced Server

Microsoft® Windows NT™ Advanced Server es un sistema operativo para computadoras (ordenadores) personales que está diseñado para uso en servidores de red de área local (LAN). Posee la potencia, la manejabilidad y la capacidad de ampliación de Windows NT™. También incluye funciones adicionales, como la administración centralizada de la seguridad y características más avanzadas de tolerancia a fallos, haciendo de él un sistema operativo idóneo para servidores de red.

Windows NT Advanced Server es a la vez un sistema operativo para computadoras y un sistema operativo para red. Debido a que lleva incorporadas las funciones de red, las redes de Windows NT Advanced Server se integran de forma óptima con el sistema operativo básico, facilitando el uso y la administración de las funciones.

Este capítulo ofrece un resumen de las funciones de Windows NT Advanced Server y explica su funcionamiento en relación a otros productos de software para red fabricados por Microsoft. También describe la finalidad de este manual y el modo más eficaz de utilizarlo.

Descripción general de Windows NT Advanced Server

Windows NT Advanced Server es un sistema operativo para servidores, ampliable e independiente de plataforma. Puede ejecutarse en sistemas basados en procesadores Intel x86, RISC y DEC® Alpha, ofreciendo al usuario mayor libertad en la selección de sistemas informáticos. Es ampliable a sistemas de multiproceso simétrico, lo que permite incorporar procesadores adicionales cuando se desee aumentar el rendimiento.

Internamente posee una arquitectura de 32 bits. Su modelo de memoria lineal de 32 bits elimina los segmentos de memoria de 64 KB y la barrera de 640 KB de MS-DOS®. Posee múltiples *threads* (subprocesos) de ejecución, lo que permite utilizar aplicaciones más potentes. La protección de la memoria garantiza la estabilidad mediante la asignación de áreas de memoria independientes para el sistema operativo y para las aplicaciones, con el fin de impedir la alteración de los datos. La capacidad de multitarea preemptiva permite al sistema operativo asignar tiempo de proceso a cada aplicación de forma eficaz.

Windows NT Advanced Server incluye, asimismo, diversas funciones de red, que se describen brevemente en las siguientes secciones y con más detalle en capítulos posteriores de este manual.

Arquitectura de redes abiertas

Windows NT Advanced Server es compatible con los estándares NDIS (Especificación de la interfaz del controlador de red) y TDI (Interfaz del controlador de transporte). NDIS es una interfaz estándar para comunicación entre controladores de tarjetas adaptadoras de red y protocolos de red. NDIS le permite combinar y coordinar tarjetas y protocolos de red sin que sea necesario disponer de una versión diferente del protocolo de red para cada tipo de tarjeta. Permite también utilizar varios protocolos en una misma tarjeta de red. Con Windows NT Advanced Server se suministran cuatro protocolos compatibles con el estándar NDIS: NetBEUI, TCP/IP, Microsoft NWLINK y DLC (Control de vínculos de datos). La interfaz TDI se comunica entre el protocolo de red y el software de red de alto nivel (como el servidor y el redirector). TDI elimina la necesidad de que el redirector y el servidor se comuniquen directamente con los protocolos de red, o de tener información de los mismos, permitiendo de esta forma utilizar protocolos, servidores o redirectores diferentes con Windows NT Advanced Server. También es compatible con aplicaciones de RPC (Llamada a procedimiento remoto), aplicaciones de sistema de entrada/salida básico de red (NetBIOS) y aplicaciones con Sockets de Windows.

Instalación desde la red

Se puede instalar Windows NT en estaciones de trabajo a través de la red, en lugar de utilizar disquetes o discos CD-ROM para cada estación. Este proceso es mucho más fácil ya que no necesita mover el medio de instalación de una computadora (ordenador) a otra.

Seguridad incorporada

Windows NT Advanced Server incorpora la seguridad en el sistema operativo. El control de acceso discrecional le permite asignar permisos a archivos individuales. El concepto de derechos de usuario le ofrece un sistema de control discrecional de las funciones básicas del sistema, como establecer la hora o apagar la computadora. Se incluyen, asimismo, funciones completas de auditoría.

Administración centralizada de la seguridad

Windows NT Advanced Server permite crear dominios y establecer relaciones de confianza, con el fin de centralizar las cuentas de usuario de la red y otro tipo de información de seguridad, facilitando el uso y la administración de la red. Con una administración centralizada de la seguridad, sólo es necesario administrar una cuenta por cada usuario. Dicha cuenta permite al usuario acceder a todos los recursos de la red.

Registro de configuración

Windows NT Advanced Server y Windows NT mantienen una base de datos denominada *registro de configuración* o simplemente *registro*. Esta base de datos contiene información acerca del sistema operativo, de la computadora (ordenador) y de los usuarios que anteriormente hayan iniciado sesiones en esta computadora. Las aplicaciones que detecten la presencia de Windows NT podrán almacenar la información de inicialización en el registro.

El registro reemplaza la necesidad de separar los archivos de configuración como CONFIG.SYS, AUTOEXEC.BAT, LANMAN.INI, WIN.INI y PROTOCOL.INI. Sin embargo, para ser compatibles con aplicaciones escritas para utilizar CONFIG.SYS y AUTOEXEC.BAT, Windows NT automáticamente mantiene y usa versiones de estos archivos que contienen solamente la información de la aplicación.

Administración de las estaciones de trabajo de los usuarios

Los perfiles de usuario de Windows NT Advanced Server le permiten proporcionar mayor facilidad de uso a los usuarios y al mismo tiempo restringir sus actividades en las estaciones de trabajo. Si desea utilizar perfiles para aumentar la productividad de los usuarios, puede guardar en los servidores un perfil con la configuración y las preferencias de los usuarios, tales como las conexiones de red, los grupos de programas e incluso los colores de la pantalla. Este perfil se utilizará cada vez que el usuario inicie una sesión en cualquier estación de trabajo con Windows NT, de forma que el entorno definido por el usuario le siga de una estación de trabajo a otra. Si desea utilizar los perfiles de usuario para limitar las actividades de los usuarios deberá agregar restricciones al perfil, como por ejemplo, impedir que el usuario cambie los grupos y los elementos de programa que haya definido, o inhabilitar parte de la interfaz de Windows NT cuando el usuario haya iniciado una sesión.

Administración de impresión en red mejorada

Windows NT incorpora una interfaz mejorada del Administrador de impresión que simplifica los procedimientos de instalación y administración de las impresoras que deben realizar los administradores, y que facilita las operaciones de examinación y conexión de impresoras que deben realizar los usuarios. Los usuarios de las estaciones de trabajo de Windows NT que se conecten a impresoras compartidas por computadoras (ordenadores) en las que se esté ejecutando Windows NT Advanced Server no necesitarán disponer de controladores de impresora instalados en la propia estación de trabajo. Windows NT Advanced Server es completamente compatible con impresoras que disponen de interfaz de red (como la Hewlett-Packard® LaserJet® IIIsi), que cuentan con tarjeta adaptadora de red incorporada, y que se conectan directamente al cable de la red y no a un puerto serie o paralelo del servidor.

Copia de seguridad en cinta

Windows NT incluye una utilidad de copia de seguridad en cinta, que permite hacer copias de seguridad centralizadas de los discos duros de las computadoras (ordenadores) en red, incluyendo servidores de Microsoft LAN Manager 2.x, estaciones de trabajo con Windows NT y computadoras con Windows™ para Trabajo en grupo, así como servidores en los que se esté ejecutando Windows NT Advanced Server.

Monitorización del rendimiento

Windows NT Advanced Server incluye también una aplicación que permite monitorizar el rendimiento. Esta herramienta puede utilizarse para observar, representar gráficamente y registrar cientos de datos estadísticos acerca de tipos específicos de rendimiento, agrupados en categorías generales tales como tráfico entre servidores de la red, rendimiento de los discos, uso de los procesadores, y estadísticas de los servidores y las estaciones de trabajo.

El Monitor de sistema le permite supervisar simultáneamente el rendimiento de un gran número de computadoras remotas, de forma que pueda controlar y comparar el rendimiento y el uso de un gran número de servidores.

Seguimiento de la actividad de la red

Windows NT Advanced Server proporciona numerosas herramientas para realizar el seguimiento de la actividad y el uso de la red. Puede observar a los servidores y examinar qué recursos están compartiendo; ver qué usuarios están conectados a un servidor de la red y observar qué archivos tienen abiertos; registrar y ver las anotaciones de auditoría de seguridad; mantener registros de error exhaustivos; y especificar las alertas que se deben enviar a los administradores en caso de que se produzcan determinados sucesos. Si su red utiliza el protocolo TCP/IP, podrá utilizar también la utilidad de administración SNMP, suministrada con Windows NT Advanced Server.

Administración remota

Todas las funciones administrativas de la red, incluyendo la administración de servidores, la administración de seguridad, la administración de impresoras y la monitorización del rendimiento, pueden realizarse de forma remota. Puede utilizarse una computadora de la red para monitorizar las actividades de cualquier servidor en la misma.

Diferencias entre Windows NT Advanced Server y Windows NT

Windows NT Advanced Server engloba a Windows NT. Windows NT Advanced Server incluye todas las características y funciones de Windows NT, pero incorpora, además, diversas mejoras que lo hacen idóneo para uso en servidores de red.

La razón más importante para elegir Windows NT Advanced Server es la posibilidad de utilizar dominios y relaciones de confianza para centralizar la administración de la seguridad. Un *dominio* es un grupo de servidores que comparten una base de datos de cuentas de usuario y de grupo, y planes de seguridad. La información de la cuenta de un usuario sólo debe suministrarse una vez para que todos los servidores del dominio reconozcan la cuenta y permitan el acceso a dicho usuario.

Asimismo, podrá crear *relaciones de confianza* entre dominios. A través de una relación de confianza, los servidores en un dominio reconocen y permiten el acceso a cuentas de otro dominio. Si diseña su red teniendo presentes los dominios y las relaciones de confianza, tendrá que crear sólo una cuenta para cada usuario. Esta cuenta permite al usuario acceder a todos los recursos de la red. Esto facilita la administración de la red, ya que sólo es necesario mantener una cuenta para cada usuario. El acceso de la red por los usuarios resulta más sencillo, ya que únicamente deberán recordar una contraseña.

Otra característica de Windows NT Advanced Server es la posibilidad de usar estrategias de *tolerancia a fallos avanzada*, como disco espejo (RAID nivel 1) y banda de disco con paridad (RAID nivel 5) en los servidores de la red. El proceso de disco espejo consiste en escribir la información de un disco duro del servidor en dos discos que mantienen conjuntos idénticos de información. Si se produce un fallo en uno de los discos, el servidor pasa automáticamente al otro. La banda de disco con paridad es una técnica de tolerancia a fallos más avanzada y eficaz en la que cada volumen lógico de datos se reparte entre varios discos. Si se produce un fallo en uno de los discos, la información almacenada puede regenerarse utilizando la información de datos y de paridad del resto de los discos.

Windows NT Advanced Server permite realizar la *duplicación de directorios* en la que un servidor actúa como servidor principal de un árbol de directorios específico. Puede designar como importadoras del árbol de directorios a otras computadoras (ordenadores). De este modo, cuando se realicen cambios en los archivos del árbol del servidor principal, Windows NT Advanced Server propagará los cambios a las computadoras importadoras. La duplicación de archivos permite la distribución automática de archivos a gran número de computadoras en la red, garantizando que dichos archivos siempre estarán actualizados.

Windows NT Advanced Server también le permite realizar el almacenamiento centralizado de entornos de usuarios, denominados *perfiles*, de manera que un usuario disponga de los mismos grupos de programas, elementos de programas y conexiones de red automáticas, independientemente de la estación de trabajo en la que el usuario esté trabajando. Si la red requiere un nivel estricto de seguridad, también puede utilizar esta característica para impedir que los usuarios cambien el entorno de sus propias estaciones de trabajo, asegurando de esta forma de que sólo puedan utilizar los componentes del sistema operativo y aplicaciones que haya autorizado el administrador.

Con Windows NT Advanced Server se incluyen otros dos componentes: Servicios para Macintosh® de Windows NT y Servicio de acceso remoto de Windows NT. Estos componentes no están disponibles en las estaciones de trabajo de Windows NT. Los Servicios para Macintosh de Windows NT permiten al servidor comunicarse con las estaciones de trabajo tipo Macintosh en la red. El Servicio de acceso remoto de Windows NT proporciona acceso a la red a estaciones de trabajo conectadas vía módem en lugar de a través de cable de red.

Funcionamiento de Windows NT Advanced Server con otro software de red

Windows NT Advanced Server está diseñado para uso en servidores de grandes redes. Funciona de forma óptima con otros sistemas operativos de red fabricados por Microsoft.

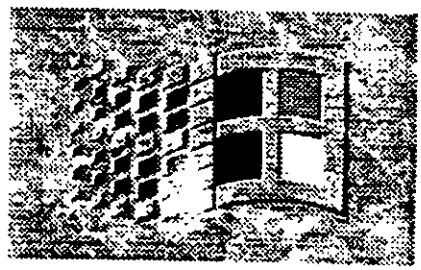
Windows NT es el sistema operativo más adecuado para los clientes que precisen altos rendimientos de la red. Windows NT está diseñado para usuarios avanzados desarrolladores de software y para aplicaciones críticas (al igual que Windows NT Advanced Server, Windows NT admite el multiproceso simétrico). Windows NT traslada al escritorio muchas de las funciones de seguridad de Windows NT Advanced Server. Al igual que en Windows NT Advanced Server, tanto la seguridad como las funciones de red están integradas en el sistema operativo.

Si desea disponer de funcionamiento de red, pero no necesita la potencia de Windows NT Advanced Server, Windows para Trabajo en grupo puede ser la solución. Windows para Trabajo en grupo se ejecuta en computadoras (ordenadores) bajo MS-DOS e incorpora funciones de red al sistema operativo Windows 3.1. Al igual que Windows NT y Windows NT Advanced Server, Windows para Trabajo en grupo incluye aplicaciones de correo electrónico y planificación de jornada que permiten aumentar la productividad de los grupos.

Windows NT Advanced Server también es compatible con los sistemas Microsoft LAN Manager 2.x. Las computadoras que se ejecuten bajo MS-DOS, Windows 3.1 y OS/2® que posean software para estaciones de trabajo LAN Manager pueden acceder a servidores en los que se ejecute Windows NT Advanced Server. Los servidores de LAN Manager 2.x (tanto en sistemas OS/2 como UNIX®) pueden funcionar con servidores en los que se esté ejecutando Windows NT Advanced Server, incluso en el mismo dominio.

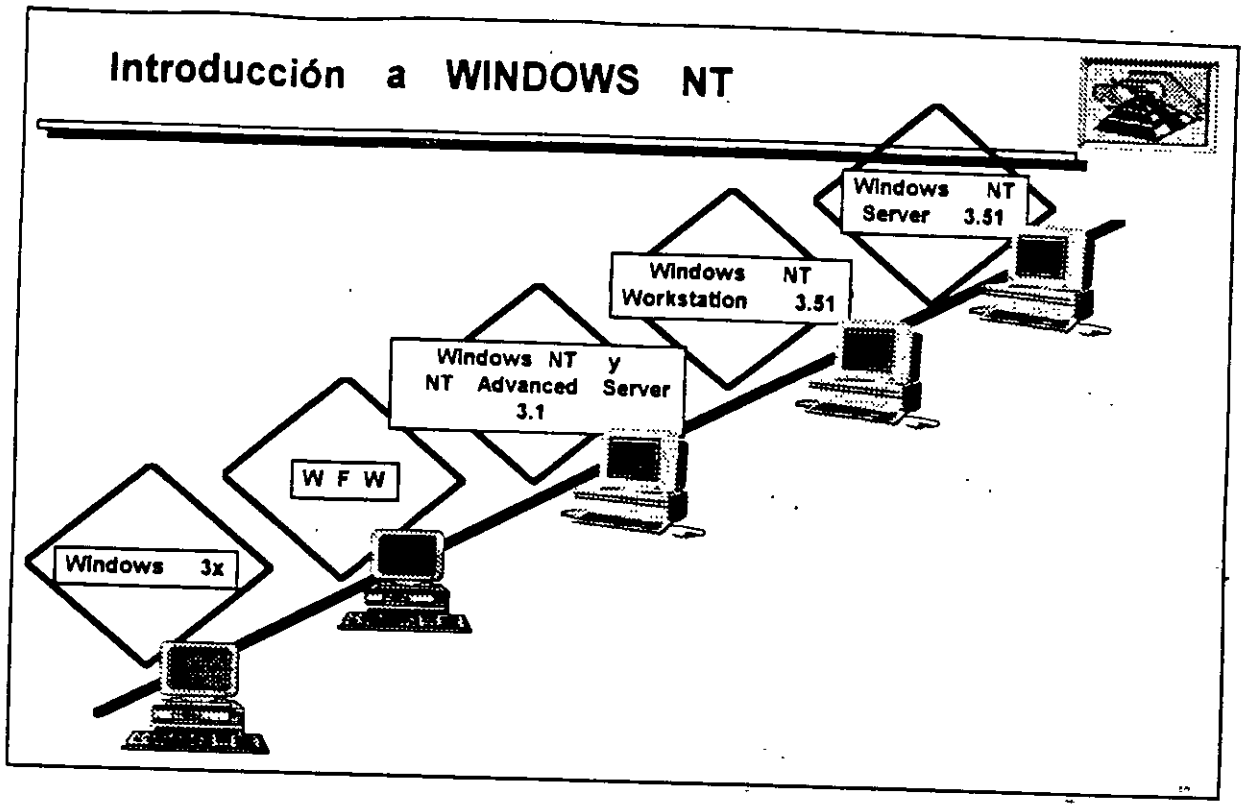
Esta familia de productos le permitirá ampliar su red de acuerdo a sus necesidades. Su red puede ser de gran tamaño, con un gran número de servidores de Windows NT Advanced Server y cientos de estaciones de trabajo con Windows NT, o de pequeña dimensión que posea una sola estación de trabajo con Windows NT Advanced Server y varias estaciones de trabajo con MS-DOS.

Introducción a WINDOWS NT



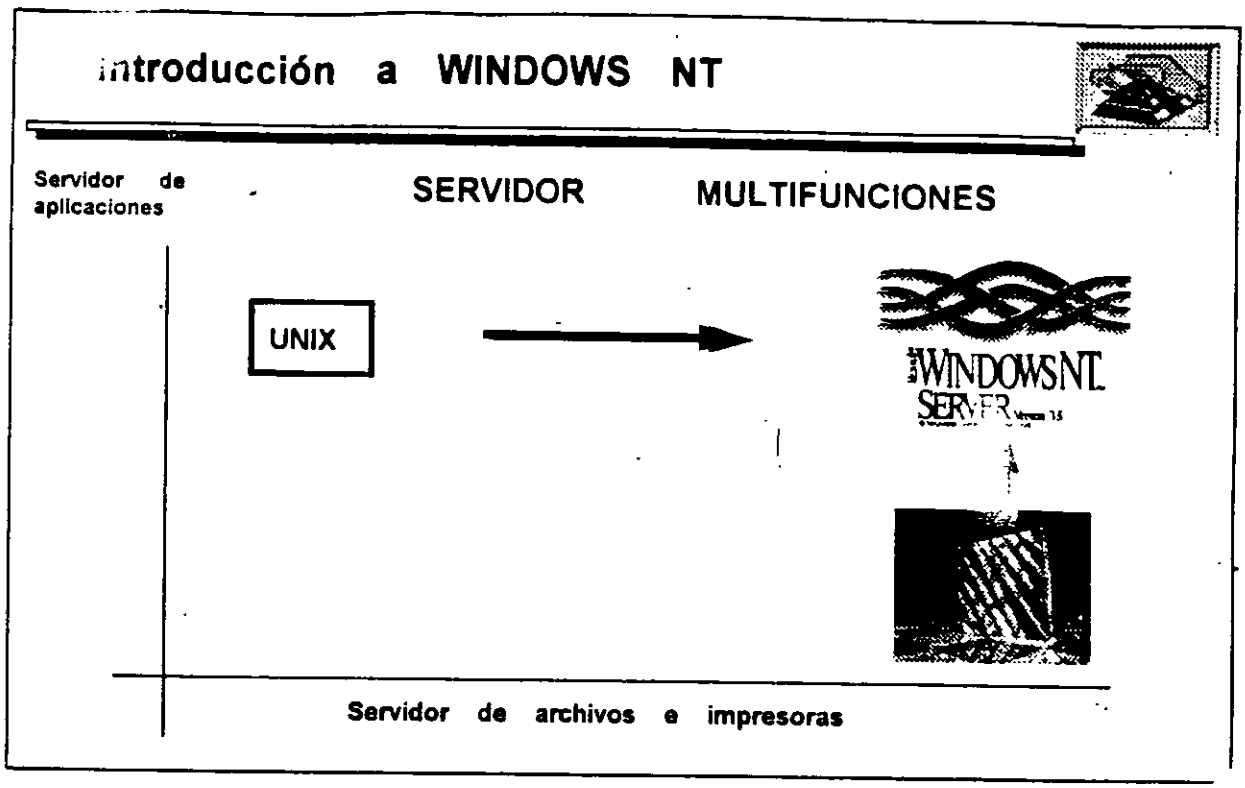
Notas:

Lámina.1.



Notas:

Lámina 2



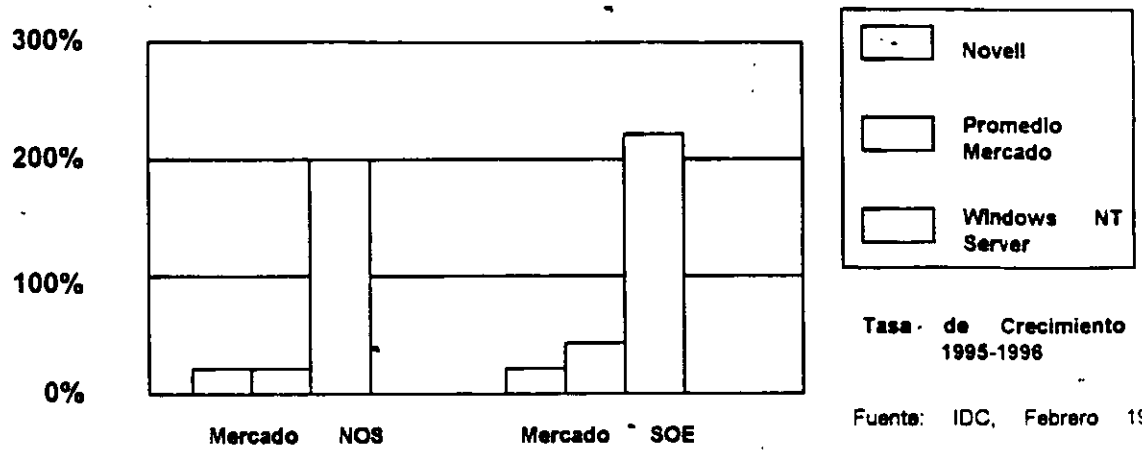
Notas:

Lámina 3

Introducción a WINDOWS NT

CRECIMIENTO DE WINDOWS NT

Network Operating System y Server Operating Evironment



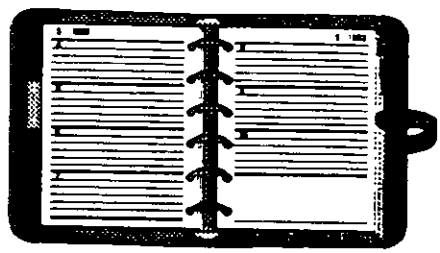
Notas:

Lámina 4

Introducción a WINDOWS NT

Revisión de Conceptos

- RED
- COMPONENTES
- TOPOLOGIAS
- PROTOCOLOS
- S.O.
- MODELO DE REFE. ICIA ISO-OSI



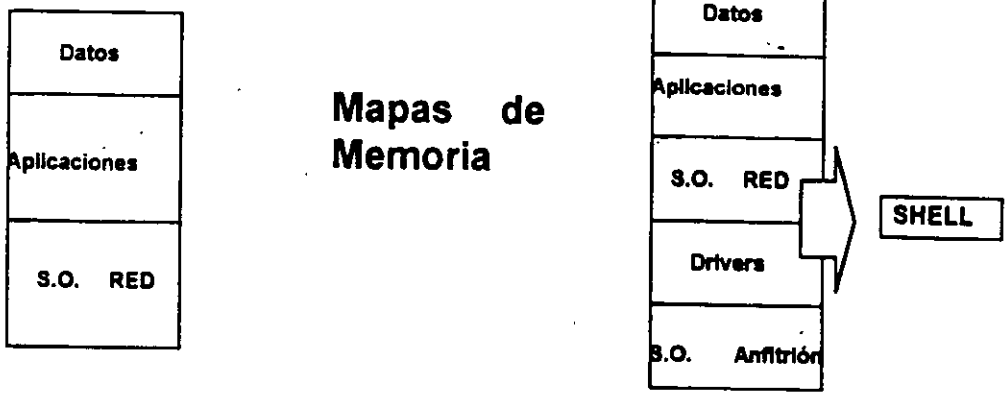
Notas:

Lámina 5.

Introducción a WINDOWS NT

SERVIDORES

Estaciones de trabajo



Notas:

Lámina 6.

Introducción a WINDOWS NT

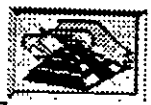
Características de WINDOWS NT

- Sistema operativo de 32 Bits
- Multiplataforma :
  - Intel 386,486, Pentium y superiores
  - MIPS R4x00
  - Digital Alpha AXP
- Arquitectura Cliente-Servidor
- Autodetección de hardware
- Escalable
- Conectividad
- Multitareas
- Multiproceso (Simple o simétrico)

Notas:

Lámina 7.

Introducción a WINDOWS NT



Características de WINDOWS NT

- Seguridad
  - Bandas de disco
  - Soporte RAID 5
  - Doble escritura en discos y duplicación de unidades
  - Soporte UPS
  - Soporte de copias de seguridad en cinta
  - Nivel de seguridad C2
- Escrito en C y código máquina
- Basado en Microkernell
- Sistema de archivos: NTFS, HPFS, FAT
- Modelo de Memoria Lineal de 32 Bits
- Multiples Threads (subprocesos) de ejecución

Notas:

Lámina 8.

Introducción a WINDOWS NT

Características de WINDOWS NT

Requerimientos del sistema

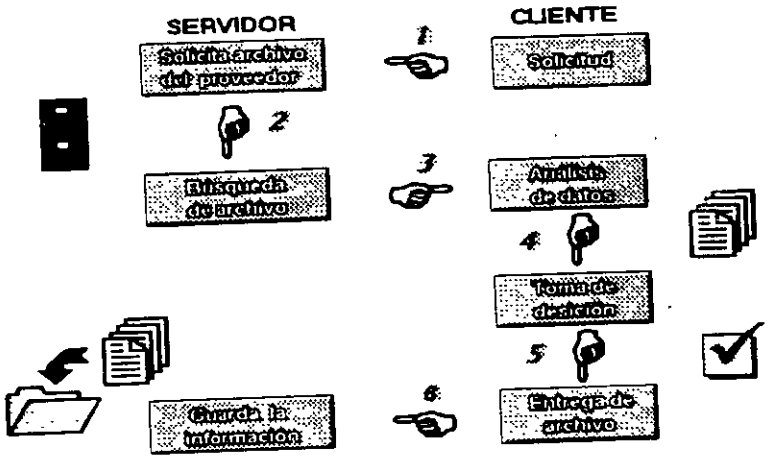
- Microprocesador 386/25 o superior o sistema basado en RISC
- 16 Mb de memoria
- Unidad CD-ROM recomendada
- Unidad e discos de alta densidad
- 90 Mb e espacio en disco (110 Mb para sistemas RIS
- Video GA
- Tarjeta de RED
- Mouse

Notas:

Lámina 9

Introducción a WINDOWS NT

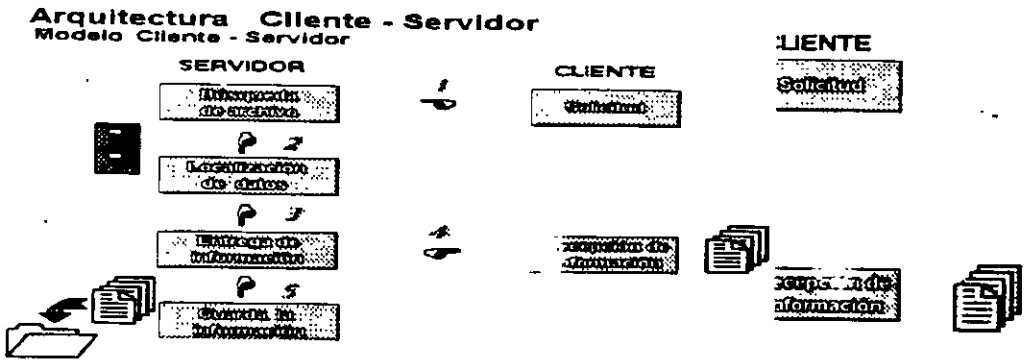
Arquitectura Cliente-Servidor.
Modelo Tradicional



Notas:

Introducción a WINDOWS NT

Arquitectura Cliente-Servidor.



Nota:

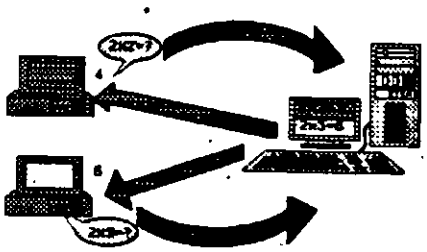
Lámina 11

Introducción a WINDOWS NT

Arquitectura Cliente-Servidor.

El cliente hace una petición

El servidor procesa y envia el resultado



Notas:

Lámina 12

Introducción a WINDOWS NT

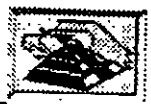
Componentes del Sistema Operativo de RED

- Software del sistema operativo
- Software del cliente
- Herramientas de migración
- Utilidades de administración
- Conectividad Macintosh
- Carga remota de programas para sistemas de clientes sin disco
- Unidades de dispositivos
- Protocolos (TCP/IP, IPX/SPX,NetBEUI, AFP,DLC)
- Servicio de acceso remoto RAS, a través de X.25, ISDN y lineas de teléfono estandar

Notas:

Lámina 13

Introducción a WINDOWS NT



Interacción de Sistemas Operativos

- Servidores
  - Interactua con Apple Talk, Digital PATHWORKS, IBM Lan Server, Redes IBM SNA, MS Lan Manager, WFW, Netware de Novell, Redes NFS, Redes TCP/IP, RAS a través de ISDN, X25 y lineas standar de telefonia.

- Estaciones de trabajo
  - Windows 3.x, Windows para Grupos de Trabajo, Windows 95 Windows NT Workstation, MS-DOS, OS/2, Macintosh y Unix

Notas:

Lámina 14

Introducción a WINDOWS NT

Características de WINDOWS NT

Complemento de Windows NT

- BackOffice:
  - SQL Server
  - MS Mail
  - SNA
  - SMS

Notas:

Lámina 15

INSTALACIÓN Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

2.- INSTALACIÓN DE WINDOWS NT

Mayo de 1996.

Elección de controladores y protocolos de red

Cuando esté instalando Windows NT o Windows NT Advanced Server en su red, deberá elegir el tipo de controladores de tarjeta adaptadora de red y de protocolos que utilizará. Debido a la arquitectura abierta de los productos para Windows NT, podrá disfrutar de una gran flexibilidad a la hora de tomar esta decisión. Windows NT admite los estándares NDIS (Especificación de interfaz de controlador de red) y TDI (Interfaz de controlador de transporte). Estos estándares permiten a Windows NT comunicarse con muchos otros productos de red, y le ofrece la posibilidad de elegir entre una amplia variedad de tarjetas adaptadoras y protocolos para la red.

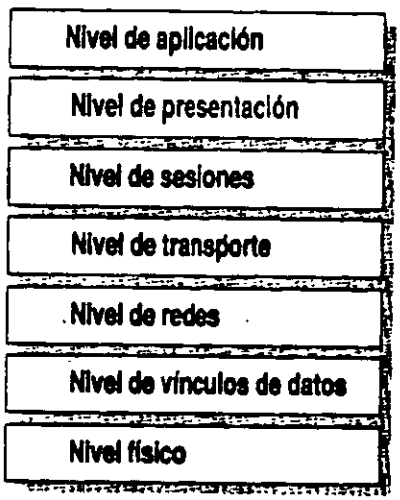
Windows NT y Windows NT Advanced Server incorporan además una versión de STREAMS®, el entorno y la interfaz de protocolos desarrollado originariamente para funcionar sobre UNIX System V versión 4.0. La incorporación de un entorno compatible con STREAMS significa que los protocolos desarrollados inicialmente para STREAMS bajo UNIX podrán trasladarse fácilmente a Windows NT.

Antes de profundizar sobre los protocolos y controladores específicos que admite Windows NT, es conveniente comprender tanto el modelo de referencia OSI (Interconexión de sistemas abiertos) como la función que desempeñan los protocolos de transporte y los controladores de tarjetas de red. Si ya conoce el significado de estos términos, puede acudir directamente a la sección "Ventajas de NDIS", ~~más adelante en este capítulo~~.

Significado del modelo de referencia OSI

En 1978, la Organización Internacional de Normalización (International Organization for Standardization [ISO]) elaboró un modelo para la interconexión de computadoras (ordenadores) en red denominado *modelo de referencia para la Interconexión de sistemas abiertos*. Este modelo describe el flujo de datos dentro de una red, desde las conexiones físicas hasta el nivel superior, es decir, las aplicaciones que utilizan los usuarios finales.

El modelo de referencia OSI consta de 7 niveles, como se muestra en la figura siguiente. El nivel más bajo, conocido como nivel físico, es donde los bits de datos se transfieren físicamente al cable. El nivel más alto es el de aplicación, que corresponde a la presentación de las aplicaciones a los usuarios.



Físico—El nivel físico es responsable de la transferencia de bits de una computadora (ordenador) a otra. Se encarga de regular la transmisión de una secuencia de bits a través de un medio físico. Este nivel define el modo en que se conecta el cable a la tarjeta adaptadora de red y la técnica de transmisión empleada para enviar los datos a través del cable. También define la sincronización de bits y las operaciones de comprobación.

Vínculos de datos—El nivel de vínculos de datos empaqueta los bits sin procesar procedentes del nivel físico, agrupándolos en *tramas*. Una trama es un paquete lógico estructurado en el cual pueden colocarse datos. El nivel de vínculos de datos es responsable de transferir tramas de una computadora a otra, sin errores. Una vez que el nivel de vínculos de datos envía una trama, queda esperando una aceptación o acuse de recibo procedente de la computadora destinataria. Las tramas para las cuales no se recibe una aceptación vuelven a enviarse.

Redes—El nivel de redes direcciona los mensajes y traduce las direcciones y nombres lógicos, convirtiéndolos en direcciones físicas. También determina la ruta a través de la red entre la computadora de origen y la de destino, y administra aspectos asociados a la red como la conmutación, el encaminamiento y el control de la congestión de paquetes de datos.

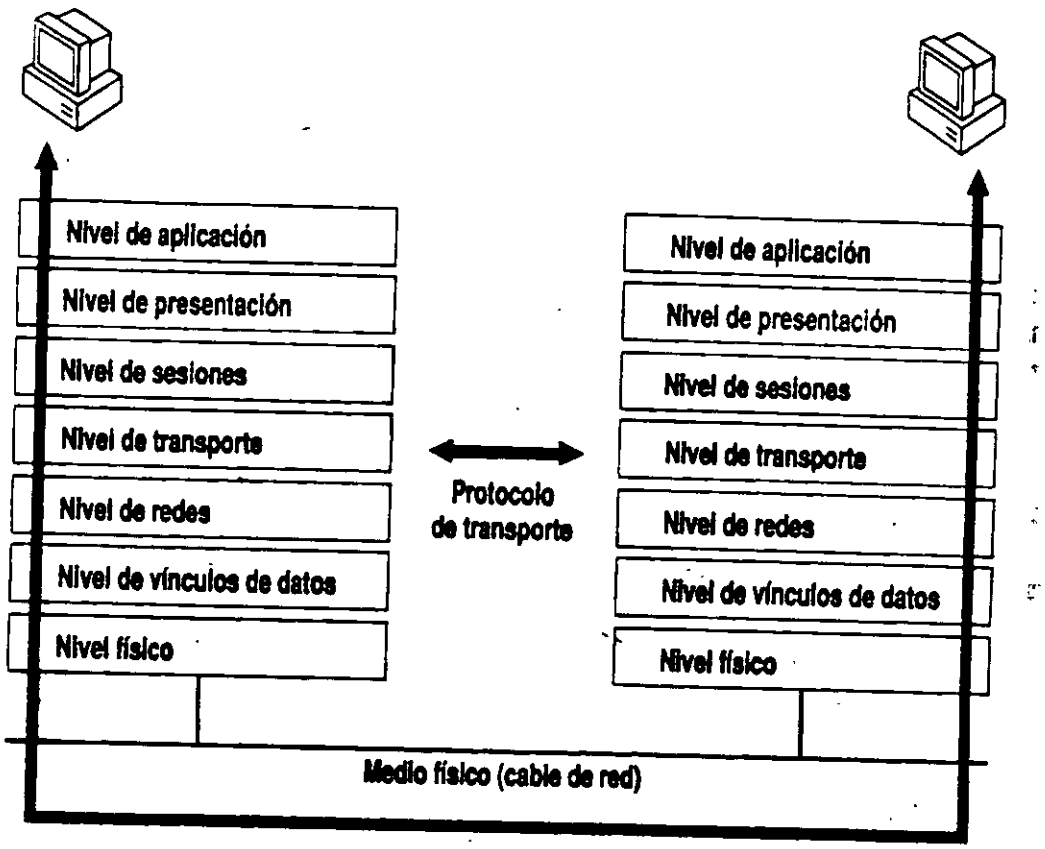
Transporte—El nivel de transporte es responsable de detectar y resolver errores, con el fin de garantizar la fiabilidad en la entrega de los mensajes. También se encarga de volver a empaquetar los mensajes cuando es necesario, dividiendo los mensajes de gran longitud en mensajes más cortos para su transmisión y reconstruyendo posteriormente, en el extremo receptor, el mensaje original a partir de los paquetes más pequeños. El nivel de transporte del extremo receptor se ocupa también de enviar la aceptación o acuse de recibo.

Sesiones—El nivel de sesiones permite a dos aplicaciones situadas en distintas computadoras establecer, utilizar y terminar una sesión. Este nivel establece el control del diálogo entre las dos computadoras que participan en una sesión, regulando cuál de los dos extremos transmite, cuándo lo hace y durante cuánto tiempo.

Presentación— El nivel de presentación traduce los datos desde el nivel de aplicación hasta un formato intermedio. Este nivel se encarga también de cuestiones relacionadas con la seguridad, proporcionando servicios como el cifrado de datos o la compresión de la información, para que se transmitan menos bits a través de la red.

Aplicación—El nivel de aplicación es el que permite a las aplicaciones de usuario final acceder a los servicios de la red.

Cuando dos computadoras (ordenadores) se comunican a través de una red, el software de cada uno de los niveles asume que se está comunicando con el nivel homólogo de la otra computadora. Por ejemplo, el nivel de transporte de una de las computadoras se comunicará con el nivel de transporte de la otra. El nivel de transporte de la primera computadora no necesita preocuparse del modo en que la comunicación atraviesa realmente los niveles inferiores de la primera computadora, recorre el medio físico y, por último, vuelve a ascender a través de los niveles inferiores de la segunda computadora.



El modelo de referencia OSI es una representación idealizada de las interconexiones en red. En realidad, pocos sistemas lo cumplen de forma estricta, pero este modelo se utiliza para la discusión y comparación de redes. En el resto de este capítulo se muestra cuáles son los componentes de Windows NT que intervienen en los distintos niveles del modelo.

Función de los protocolos y controladores de tarjetas adaptadoras

Una *tarjeta adaptadora de red* (también conocida como tarjeta de interfaz de red o NIC) es una tarjeta de hardware que se instala en una computadora (ordenador) para permitir su uso dentro de una red. La tarjeta adaptadora de red proporciona uno o varios puertos en los cuales se conecta físicamente el cable de la red. La tarjeta realiza la transmisión física de los datos de la computadora a la red y viceversa.

Toda computadora que forme parte de una red debe tener un *controlador de tarjeta adaptadora de red*, es decir, un controlador de software que gobierne el funcionamiento de la tarjeta de red. Cada controlador de tarjeta adaptadora de red está configurado expresamente para funcionar con un determinado tipo de tarjeta de red.

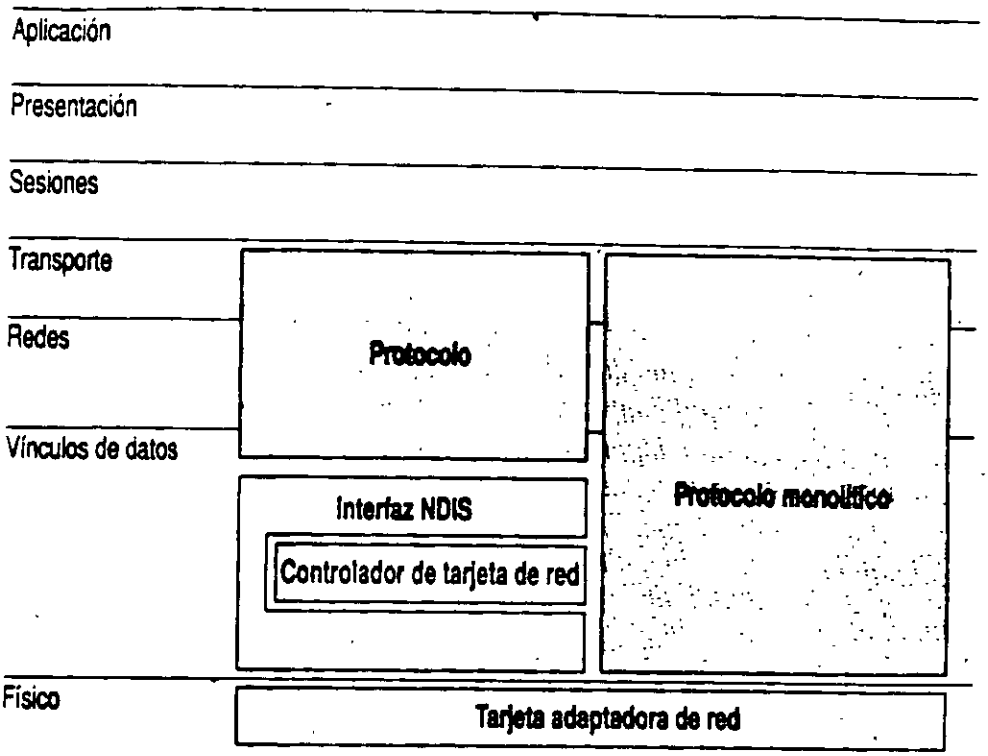
Además del controlador de tarjeta de red y de la propia tarjeta, una computadora conectada en red debe poseer también un *controlador de protocolo* (también conocido como *protocolo de transporte* o, simplemente, *protocolo*). El controlador de protocolo actúa entre el software de red de un nivel superior (por ejemplo, la estación de trabajo y el servidor) y la tarjeta adaptadora de red. El protocolo empaqueta los datos que van a enviarse a la red de tal modo que la computadora del otro extremo pueda entenderlos.

El proceso de asociar un controlador de protocolo a la tarjeta adaptadora de red con la que deberá funcionar, así como el establecimiento de un canal de comunicación entre ambos, se conoce como *vínculo*.

Para que dos computadoras se comuniquen en una red, es necesario que ambas utilicen protocolos idénticos. En ocasiones una computadora puede estar configurada para utilizar varios protocolos. En tales casos, para que dos computadoras puedan comunicarse, bastará con que ambas tengan un protocolo en común. Por ejemplo, un servidor que utilice tanto NetBEUI como TCP/IP podrá comunicarse tanto con estaciones de trabajo que utilicen únicamente NetBEUI como con aquéllas que sólo usen TCP/IP.

En algunas redes, el protocolo y el controlador de la tarjeta adaptadora de red son elementos de software independientes. En otras redes, por el contrario, un mismo elemento de software, conocido como *pila de protocolos monolítica*, desempeña las funciones tanto del protocolo como del controlador de la tarjeta adaptadora.

La siguiente ilustración muestra el modo en que estos tipos de controladores se ajustan al modelo de referencia OSI.



Windows NT y Windows NT Advanced Server admiten NDIS (versión 3.0), que permite utilizar controladores de tarjetas adaptadoras y protocolos por separado. Todos los protocolos y controladores de tarjetas de red que se suministran con Windows NT Advanced Server se ajustan al estándar NDIS.

Ventajas de NDIS

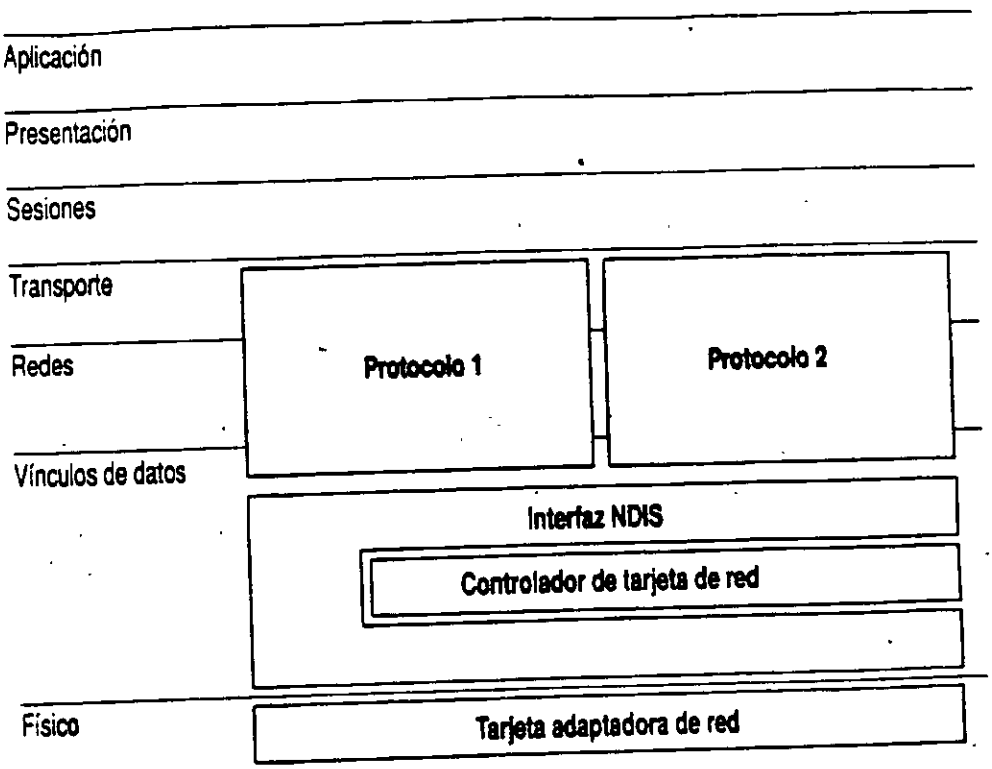
NDIS ofrece un conjunto de normas para la comunicación entre protocolos y controladores de tarjetas adaptadoras. Así, en cualquier estación de trabajo podrá utilizarse cualquier combinación de controladores de protocolo compatibles con NDIS junto con cualquier controlador de tarjeta adaptadora de red compatible con NDIS. (Todos los controladores de protocolos y de tarjetas adaptadoras de red que se suministran con Windows NT y con Windows NT Advanced Server se ajustan al estándar NDIS.)

Es probable que las computadoras (ordenadores) existentes en su red tengan distintos tipos de tarjetas adaptadoras de red, por lo que necesitará distintos controladores de tarjetas adaptadoras de red. Gracias al estándar NDIS, podrá utilizar exactamente el mismo controlador de protocolo en todas sus estaciones de trabajo, sin la necesidad de disponer de una versión diferente del protocolo para cada tarjeta adaptadora de red, como sucedería si utilizase pilas de protocolos monolíticas.

Además, NDIS permite que varios protocolos utilicen una misma tarjeta de red. Normalmente, cuando se utiliza un protocolo monolítico con una tarjeta adaptadora de red, dicho protocolo monopoliza la tarjeta de red, impidiendo la utilización de otros protocolos con dicha tarjeta.

Cuando una computadora incorpora varios protocolos, la computadora transmite los datos utilizando primero un protocolo, después el siguiente protocolo y así sucesivamente. Cuando instale varios protocolos en una misma computadora, designará el orden en que la computadora los utilizará. El primer protocolo de esta serie suele conocerse como *protocolo principal.*

En una computadora con Windows NT, cada uno de los vínculos entre un protocolo y una tarjeta adaptadora de red tiene asignado un *número de adaptador de red local.* Por ejemplo, un protocolo unido a dos tarjetas de red necesitará dos números de adaptador de red local; dos protocolos unidos a dos tarjetas de red cada uno necesitará cuatro números de adaptador de red local. Cuando instale Windows NT en una computadora (y cuando instale tarjetas adaptadoras de red o protocolos adicionales), Windows NT asignará automáticamente números de adaptador de red local a los vínculos entre protocolos y tarjetas adaptadoras de red. Sólo necesitará cambiar estos números de adaptador de red local si tiene alguna aplicación NetBIOS que exija la utilización de un determinado número de adaptador de red local. Si necesita instrucciones para configurar los números de adaptador de red local, consulte la sección dedicada a la opción "Red" del Panel de control, en el *Manual de sistema de Windows NT Advanced Server.*



NDIS le permite enlazar dos o más protocolos a uha sola tarjeta adaptadora de red.

Elección de una tarjeta adaptadora de red

Por lo general, cada modelo específico de tarjeta adaptadora de red compatible con Windows NT o con Windows NT Advanced Server tiene asociado un controlador de tarjeta adaptadora de red. Este controlador puede ser uno de los que se incluyen con Windows NT o suministrado por el fabricante. Por lo tanto, más que elegir un controlador de tarjeta adaptadora de red, es elegir una tarjeta de red.

Cuando elija una tarjeta adaptadora de red, debe asegurarse de que la tarjeta elegida admita la arquitectura de su red (por ejemplo, Ethernet o Token-ring) y su sistema de cableado (por ejemplo, coaxial delgado o par trenzado). Además de estos factores, debe tenerse en cuenta tanto la velocidad como el costo, así como los compromisos entre ambos parámetros.

En las tarjetas adaptadoras de red, la velocidad depende principalmente del ancho del bus y de la memoria que incorpore la tarjeta. El ancho del bus de una tarjeta de red es el número de contactos que se utilizan para conectar la tarjeta al bus de la computadora (ordenador). Se obtendrá mayor rendimiento cuanto más se aproxime el ancho del bus de la tarjeta al ancho del bus interno de la computadora. La memoria incorporada en la propia tarjeta permite a ésta almacenar temporalmente las tramas que entran y salen por la red. Sin embargo, no siempre una tarjeta con más memoria constituye la opción óptima, ya que a partir de un cierto punto, las ventajas asociadas a la mayor cantidad de memoria disminuyen y es la velocidad máxima de otros componentes de la red lo que limita el rendimiento, impidiendo mejoras adicionales.

Algunas tarjetas incorporan también procesadores integrados (estas tarjetas suelen conocerse como *tarjetas inteligentes*). Sin embargo, con Windows NT las tarjetas inteligentes apenas representan una ventaja, ya que es Windows NT, con sus controladores, el que realiza la mayor parte del trabajo de procesamiento relacionado con la red.

Al considerar el costo de las tarjetas de red, reserve una parte de la inversión para adquirir tarjetas de reserva con las que reemplaza a las que fallen. Asegúrese también de que el presupuesto asignado al hardware de la red contemple el cableado, los nodos centrales, repetidores, encaminadores y otros dispositivos, además de las tarjetas, así como el costo de la mano de obra necesaria para instalarlas.

Antes de invertir en un determinado tipo de tarjeta de red, asegúrese de que exista un controlador conforme al estándar NDIS para dicha tarjeta. Además, cerciórese de que el fabricante dispone de infraestructura suficiente para atender las necesidades de su empresa. Si está tratando con un distribuidor, asegúrese de que éste posea una vía de comunicación adecuada con el fabricante de la tarjeta.

Con Windows NT y con Windows NT Advanced Server, una vez instalada una tarjeta de red en una computadora (ordenador), la instalación del controlador correspondiente resultará muy sencilla. Es suficiente con que utilice el programa de instalación o la opción "Red" del Panel de control, y con que elija el nombre de la tarjeta adaptadora de red entre las que aparecen en la lista. Si posteriormente se agregan otros protocolos, también quedarán unidos de forma automática al controlador de la tarjeta de red.

Elección de un protocolo

Microsoft ofrece cuatro protocolos para utilizar con Windows NT y con Windows NT Advanced Server: NetBEUI, TCP/IP, NWLink y DLC (Control de vínculo de datos). Debe elegir el modo en que se utilizará uno o varios de estos protocolos en su red. En las siguientes secciones se indican el uso, las ventajas y desventajas de cada uno de ellos.

Funcionamiento de NetBEUI

NetBEUI (Interfaz extendida de usuario de NetBIOS) fue presentado por primera vez por IBM en 1985. NetBEUI es un protocolo compacto, eficiente y rápido.

En 1985, cuando fue desarrollado el protocolo NetBEUI, se consideró que las redes estarían segmentadas en grupos de trabajo de entre 20 y 200 computadoras (ordenadores) y que se utilizarían pasarelas *(gateways)* para conectar cada segmento de red local con otro segmento de red local, o con una computadora central.

NetBEUI está optimizado para obtener un rendimiento muy elevado cuando se utiliza en redes locales o segmentos de redes locales departamentales. En cuanto al tráfico cursado dentro de un segmento de red local, NetBEUI es el más rápido de los protocolos suministrados con Windows NT.

La versión de NetBEUI que se entrega con Windows NT es NetBEUI 3.0. NetBEUI 3.0 corrige algunas limitaciones de versiones anteriores de NetBEUI, como las siguientes:

- NetBEUI 3.0, junto con el nivel TDI, elimina la limitación anterior de 254 sesiones por servidor en una misma tarjeta adaptadora de red.
- NetBEUI 3.0 es completamente autoajustable.
- NetBEUI 3.0 ofrece un rendimiento mucho mayor sobre vínculos lentos que las versiones anteriores de NetBEUI.

En sentido estricto, NetBEUI 3.0 no es realmente NetBEUI, sino más bien un protocolo con formato de trama de NetBIOS (NBF). NetBEUI utiliza la interfaz NetBIOS como su interfaz de nivel superior, mientras que NBF se ajusta al estándar de Interfaz de controlador de transporte (TDI). (Si desea obtener más información sobre TDI, consulte la sección "Concepto de nivel TDI" más adelante en este capítulo). No obstante, NBF es totalmente compatible e interoperable con el NetBEUI incluido en productos anteriores de red de Microsoft y, en las pantallas de Windows NT Advanced Server, se hace referencia a él como NetBEUI.

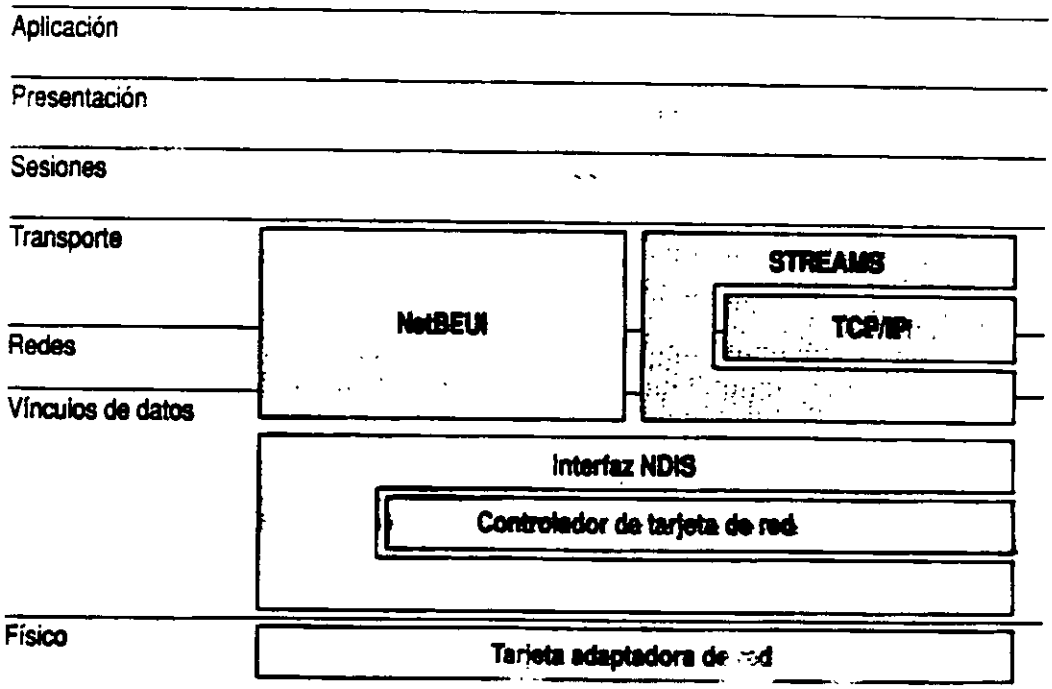
Para ver un ejemplo de cómo aprovechar las ventajas de velocidad que ofrece NetBEUI dentro de un segmento de red local, sin verse limitado por sus restricciones de encaminamiento y de funcionamiento en redes de área extensa (WANs), consulte la sección siguiente, "Estrategias para el uso de NetBEUI".

La siguiente tabla muestra un resumen de las ventajas y desventajas de NetBEUI:

Ventajas	Desventajas
Concebido expresamente para la comunicación dentro de redes locales pequeñas y, por lo tanto, muy rápido.	No admite encaminamiento.
	Su rendimiento en redes de área extensa (WANs) es pobre.
Buena protección frente a errores.	
Utiliza poca memoria.	

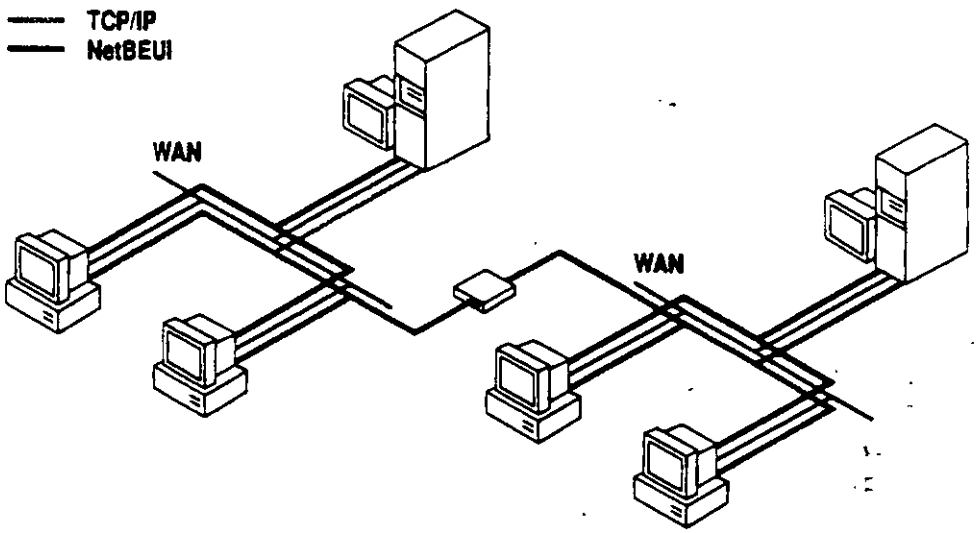
Estrategias para el uso de NetBEUI

Puesto que NetBEUI es muy rápido para comunicaciones dentro de redes locales de pequeño tamaño, pero su rendimiento es peor para las comunicaciones con redes de área extensa (WAN), un método recomendable para configurar una red es utilizar NetBEUI y otro protocolo, como TCP/IP, en cada una de las computadoras (ordenadores) que necesiten acceder a otras computadoras a través de un encaminador o una red de área extensa.



NetBEUI y TCP/IP se enlaza a una sola tarjeta adaptadora de red.

Si instala ambos protocolos en cada una de las computadoras y configura NetBEUI como el primer protocolo que deberá utilizarse, Windows NT empleará NetBEUI para la comunicación entre computadoras con Windows NT situadas dentro de cada uno de los segmentos de red local, mientras que empleará TCP/IP para las comunicaciones a través de encaminadores y con otras partes de la red de área extensa.



Funcionamiento de TCP/IP

TCP/IP son las siglas en inglés de Protocolo de control de transmisión/Protocolo Internet. Fue desarrollado a finales de los años 70, como resultado de un proyecto de investigación sobre interconexión de redes realizado por la Agencia de proyectos de investigación avanzada para la Defensa (DARPA) de Estados Unidos.

La principal ventaja y utilidad de TCP/IP es que permite comunicarse a través de redes interconectadas con distintos sistemas operativos y arquitecturas de hardware, como UNIX o computadoras (ordenadores) centrales, así como con Windows NT.

TCP/IP ofrece además compatibilidad con *Internet*, un conjunto de redes y pasarelas (*gateways*) interconectadas que vinculan numerosas universidades, empresas, organismos gubernamentales e instalaciones militares de todo el mundo.

Además, TCP/IP es necesario para poder utilizar el sistema de administración de red SNMP (Protocolo simple para la administración de redes). SNMP puede utilizarse para monitorizar cualquier computadora con Windows NT que utilice TCP/IP como su protocolo principal o como protocolo adicional.

La versión de TCP/IP desarrollada por Microsoft utiliza un entorno y una interfaz compatible con STREAMS. Windows NT admite STREAMS como interfaz entre el nivel TDI y los niveles de red inferiores..

El TCP/IP de Microsoft utiliza también la interfaz de NetBIOS, comúnmente conocido como Petición para comentarios (RFC) de NetBIOS.

Microsoft proporciona además varias utilidades de TCP/IP para la utilización de TCP/IP en Windows NT y en Windows NT Advanced Server.

La siguiente tabla muestra un resumen de las ventajas y desventajas de la utilización de TCP/IP:

Ventajas	Desventajas
Ofrece conectividad a través de distintas plataformas de hardware y sistemas operativos.	No es tan rápido como NetBEUI en redes locales de pequeño tamaño.
Permite conectarse a Internet.	
Admite encaminamiento.	
Admite SNMP.	

Funcionamiento de NWLink

NWLink es una versión compatible con NDIS del protocolo IPX/SPX, que se utiliza en las redes de Novell NetWare. Al igual que el TCP/IP que se suministra con Windows NT, NWLink utiliza la interfaz compatible con STREAMS.

NWLink es compatible con TDI, así como con NetBIOS y con Sockets de Windows, versión para Windows NT de la interfaz Sockets desarrollado originariamente para computadoras (ordenadores) con Unix.

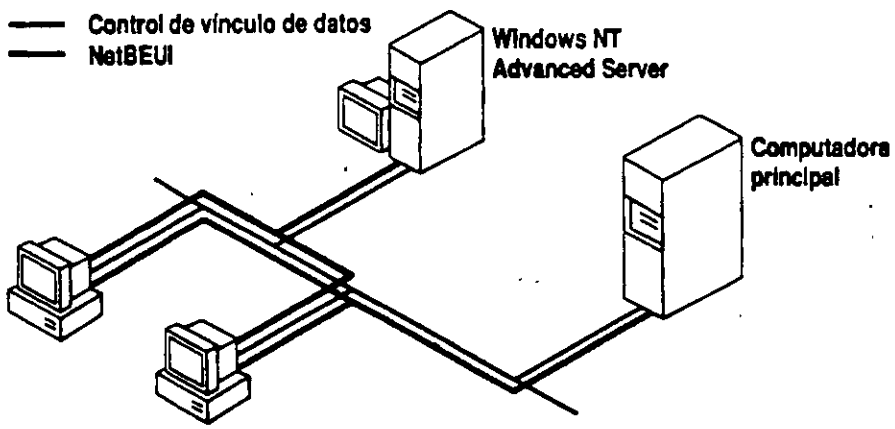
NWLink proporciona un protocolo compatible con el protocolo IPX/SPX de Novell NetWare, por lo que las computadoras con Windows NT pueden interoperar con servidores Novell NetWare. Sin embargo, NWLink no proporciona esa interoperatividad por sí solo: sigue siendo necesario ejecutar software de estación de trabajo con NetWare en una computadora con Windows NT para que ésta pueda comunicarse con servidores con NetWare.

Funcionamiento de DLC (Control de vínculo de datos)

A diferencia de NetBEUI y TCP/IP, el protocolo DLC no ha sido diseñado para servir de protocolo principal entre PCs. Por el contrario, los únicos motivos por los que puede interesar utilizar DLC con Windows NT o con Windows NT Advanced Server son los dos siguientes:

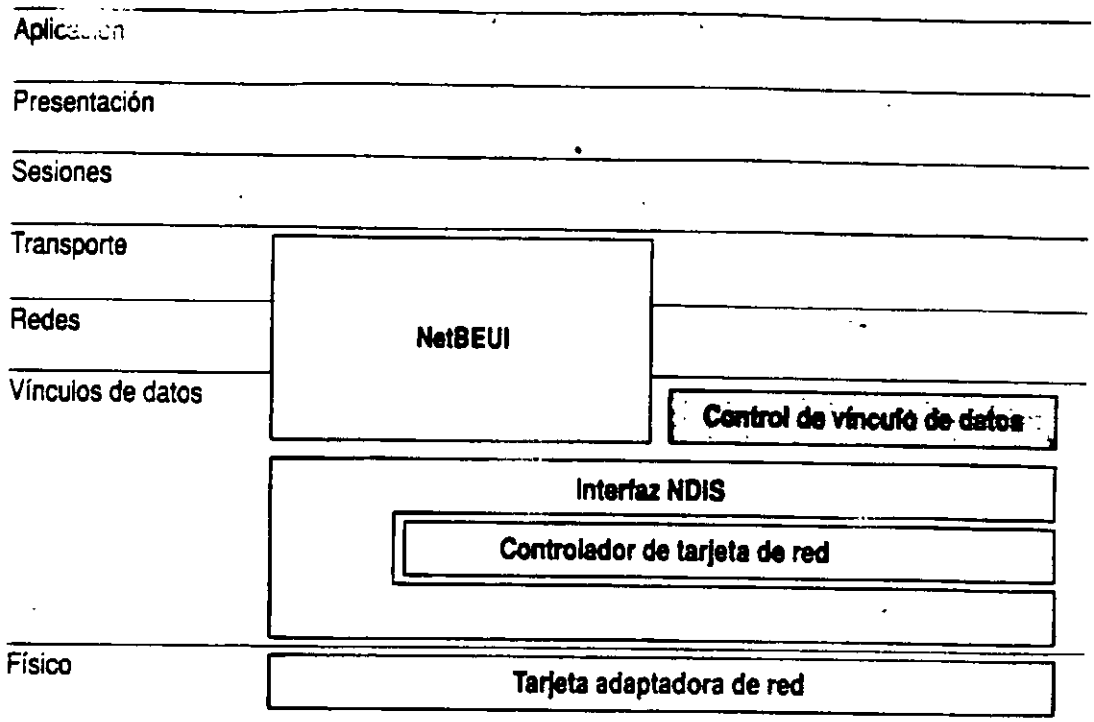
- Si necesita que las computadoras (ordenadores) con Windows NT accedan a computadoras centrales IBM®
- Si está configurando una impresora que se conecta directamente a un cable de red, en lugar de conectarse a través de un puerto serie o paralelo de un servidor de impresora

Si desea utilizar DLC para permitir la comunicación entre computadoras con Windows NT y computadoras centrales, será suficiente con que añada el protocolo DLC como protocolo adicional en cada una de las computadoras que se comunican realmente con las computadoras centrales. No es necesario que instale DLC en todas las computadoras de la red.



Cualquier estación de trabajo que ejecuta el protocolo de control de vínculo de datos puede acceder a las computadoras principales que admiten dicho control.

Para utilizar DLC con una impresora conectada a la red, por ejemplo una Hewlett-Packard Laserjet IIIsi, sólo necesita instalar DLC en la estación de trabajo con Windows NT o con Windows NT Advanced Server que actúa como servidor de impresión para dicha impresora. No es necesario que instale DLC en las computadoras que envían documentos a la impresora conectada directamente a la red. Si desea obtener más información al respecto, consulte el capítulo 6, "Uso compartido de impresoras".



A diferencia de los otros protocolos de Windows NT, como NetBEUI o TCP/IP, el protocolo DLC no se encuadra dentro de los niveles de redes o de transporte del modelo de referencia OSI, sino que ofrece a los programas de alto nivel una interfaz directa con el nivel de vínculos de datos.

La siguiente tabla muestra un resumen de las ventajas y desventajas de la utilización de DLC:

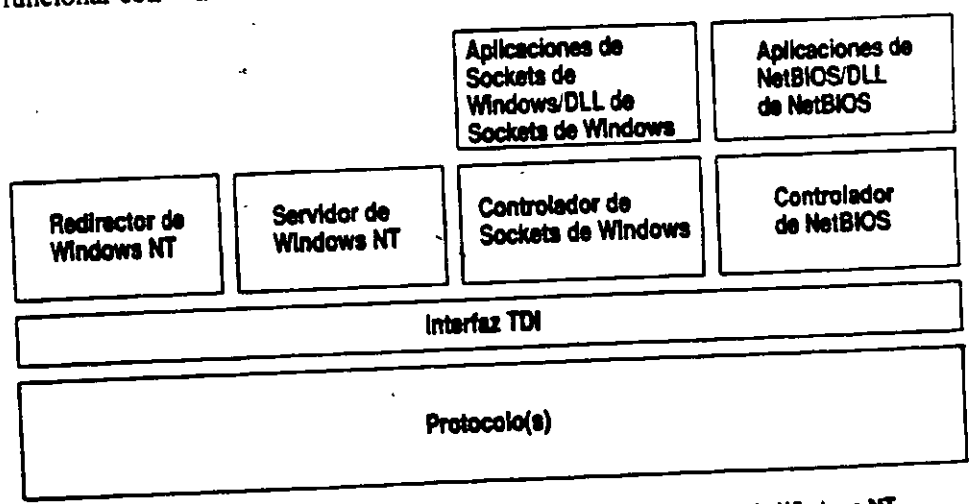
Ventajas	Desventajas
Permite a las computadoras (ordenadores) con Windows NT ejecutar software que acceda a computadoras centrales.	No suele utilizarse como protocolo principal para la comunicación de PC a PC.
Permite a las estaciones de trabajo con Windows NT actuar como servidores de impresión para impresoras conectadas directamente a la red.	

Concepto de nivel TDI

Para la comunicación entre los niveles de sesión y de transporte del modelo de referencia OSI, Microsoft ha desarrollado y admite la Interfaz de controlador de transporte (TDI). En una computadora (ordenador) con Windows NT, los procesos servidor y redirector se comunican con los protocolos de transporte utilizando la interfaz TDI.

Al igual que NDIS, TDI aumenta la versatilidad de conexión en red de Windows NT, al permitir que distintos protocolos de transporte y componentes de red de niveles superiores (como el servidor y el redirector) puedan comunicarse a través de una interfaz común. Varios protocolos diferentes que se ajusten al estándar TDI podrán cooperar con distintos componentes de niveles superiores que también admitan TDI. Cuando un redirector o un servidor realice una llamada a un transporte, se utilizará la interfaz TDI para realizar la llamada, por lo que no será necesario conocer nada acerca de los protocolos de transporte que se estén utilizando.

La incorporación de TDI en Windows NT significa que otros protocolos alternativos, o incluso redirectores o servidores alternativos, que hayan sido creados por otros fabricantes siguiendo las normas del estándar TDI, podrán funcionar con Windows NT.



Tanto el redirector y servidor de Windows NT como los Sockets de Windows y NetBIOS se comunican con los protocolos vía TDI.

El uso de TDI permite a Windows NT superar las limitaciones de anteriores productos para LAN Manager 2.x. Por ejemplo, TDI no impone ningún límite en el número de estaciones de trabajo que pueden conectarse a un servidor, mientras que LAN Manager 2.x estaba limitado a 254 conexiones de estación de trabajo en cada una de las tarjetas adaptadoras de red del servidor.

Aunque TDI es ahora la interfaz de comunicación entre los protocolos de transporte y elementos de software de nivel superior como el redirector o el servidor, también es compatible con NetBIOS. NetBIOS se ha incluido como controlador y DLL adicionales. Permite a Windows NT conservar la compatibilidad con aplicaciones de NetBIOS y ejecutar software que requiera expresamente NetBIOS. El software NetBIOS sólo se utiliza en estos casos.

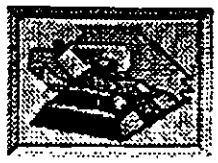
Del mismo modo, se dispone de una biblioteca de Sockets de Windows para aquellas aplicaciones que la necesiten. Sockets de Windows es una versión para Windows NT de la interfaz Sockets desarrollada originariamente para computadoras (ordenadores) con UNIX.

Configuración de RPC

Windows NT y Windows NT Advanced Server permiten utilizar aplicaciones distribuidas basadas en RPC (Llamada a procedimiento remoto). Microsoft RPC consta de un conjunto de servicios y bibliotecas de tiempo de ejecución que permiten ejecutar una aplicación distribuida bajo Windows NT. Una aplicación distribuida consta de múltiples procesos que colaboran para llevar a cabo una determinada tarea. Estos procesos pueden estar ejecutándose en una misma computadora (ordenador) o en varias diferentes.

Microsoft RPC utiliza un *proveedor de servicio de nombres* para localizar y registrar los servidores de la red. Los proveedores de servicio de nombres para Microsoft RPC deben ajustarse al estándar de NSI (Interfaz de servicio de nombres) de Microsoft RPC. NSI consta de un conjunto de funciones de la API (Interfaz de programación de aplicaciones) que permiten el acceso y la manipulación de una base de datos del servicio de nombres. Una base de datos de servicio de nombres es una base de datos que contiene entradas para servidores, para grupos y para perfiles. Microsoft RPC versión 1.0 interactúa con dos proveedores de servicio de nombres: Microsoft Localizador y el CDS (Servicio de directorio de celdas) del DCE (Entorno de computación distribuida).

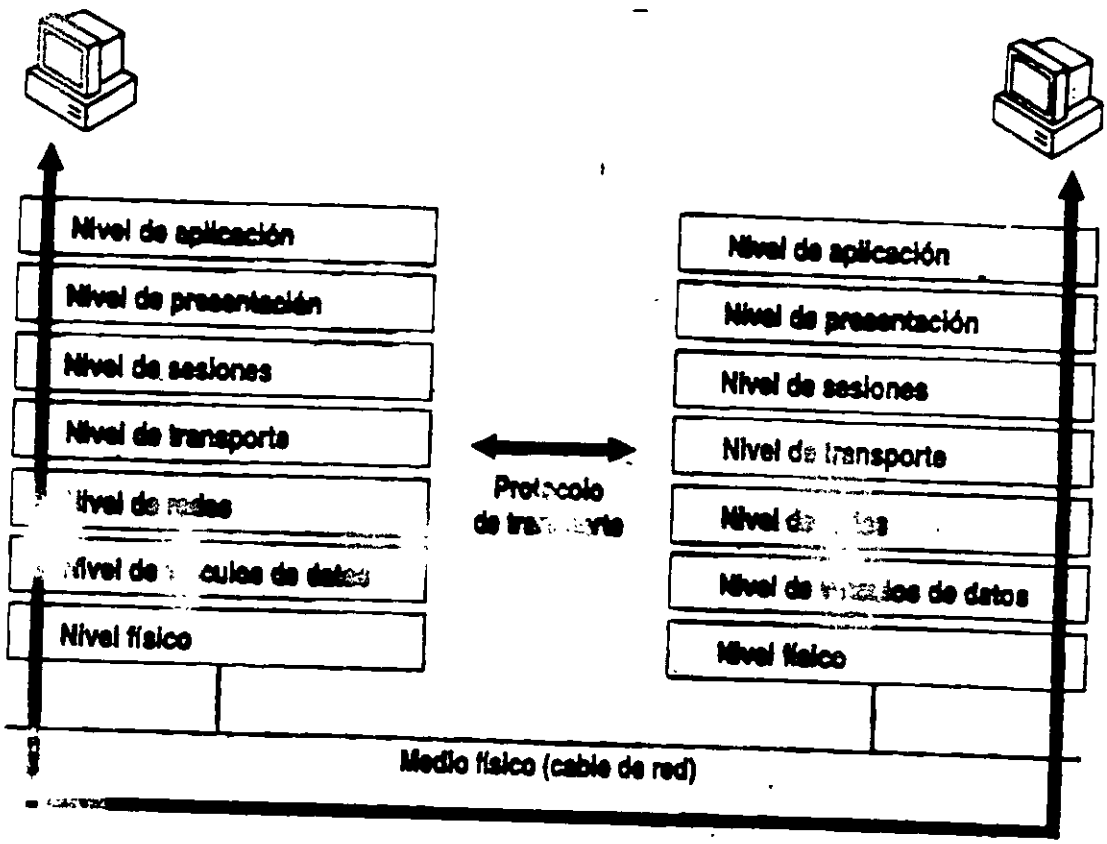
WINDOWS NT MODELO DE REFERENCIA OSI



- Nivel de aplicación
- Nivel de presentación
- Nivel de sesiones
- Nivel de transporte
- Nivel de redes
- Nivel de vínculos de datos
- Nivel físico

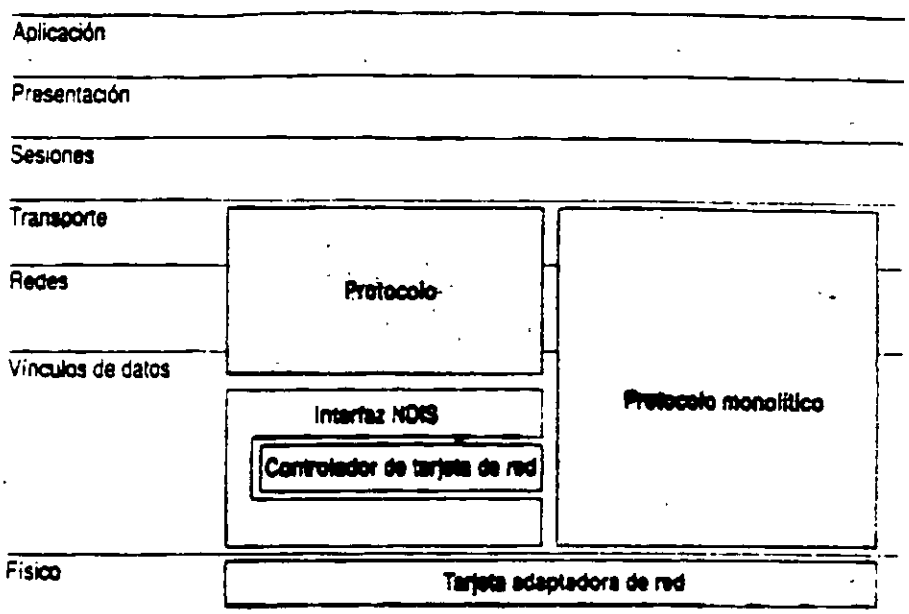
Notas:

WINDOWS NT MODELO DE REFERENCIA OSI



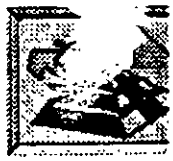
Notas:

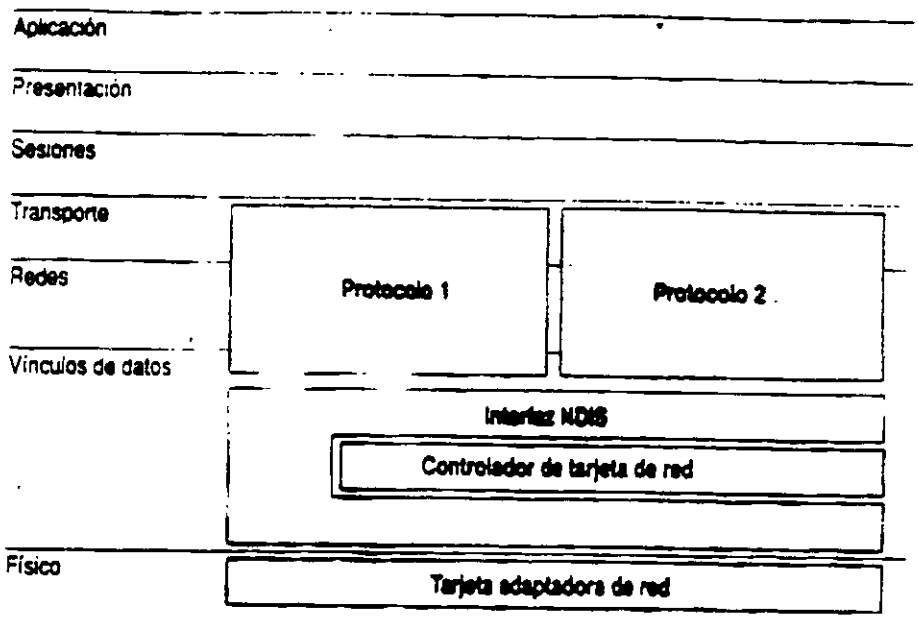
WINDOWS NT PROTOCOLO: NDIS MONOLITICO



Notas:

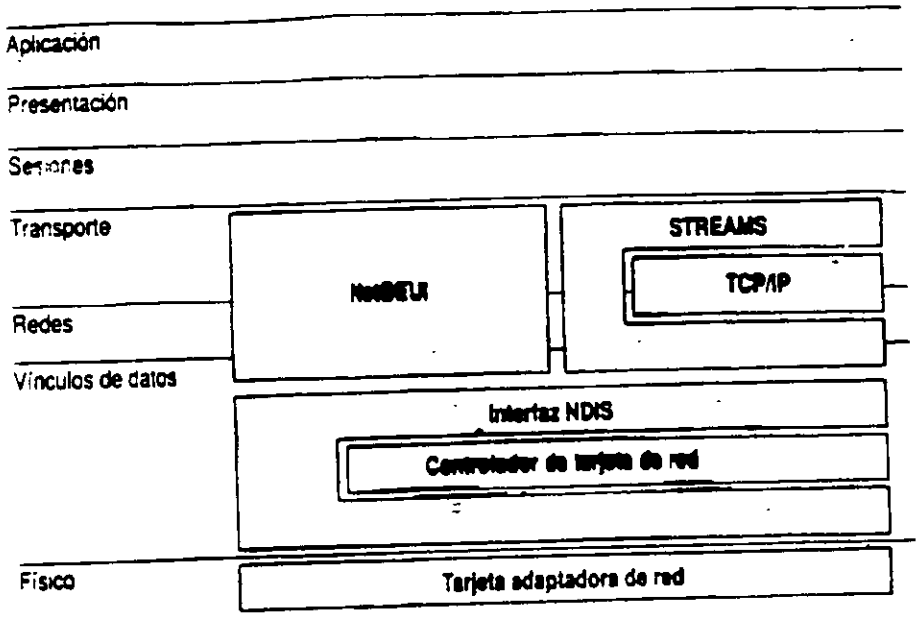
WINDOWS NT PROTOCOLO NDIS (Especificacón de interfaz de controlador de red)





Notas:

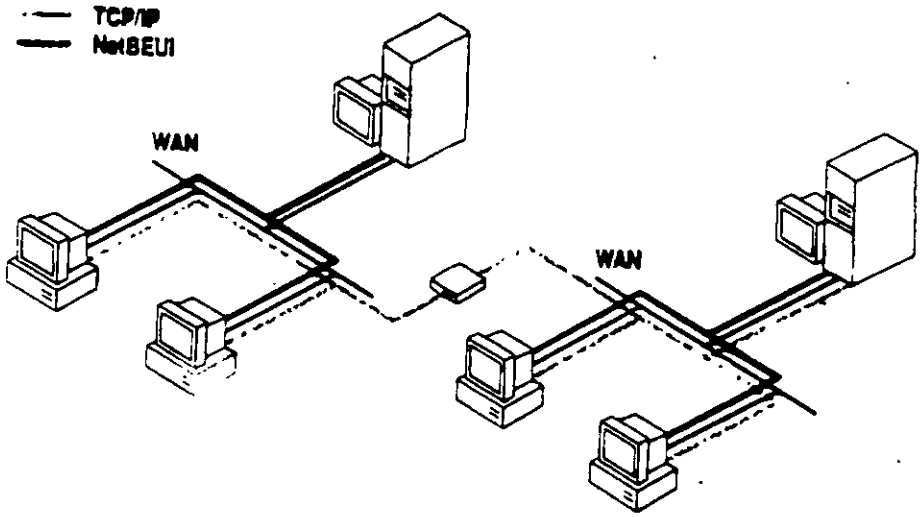
WINDOWS NT PROTOCOLO DE RED: NetBEUI (Interfaz extend de usuario NetBIOS Y TCP/IP



NetBEUI y TCP/IP se enlaza a una sola tarjeta adaptadora de red.

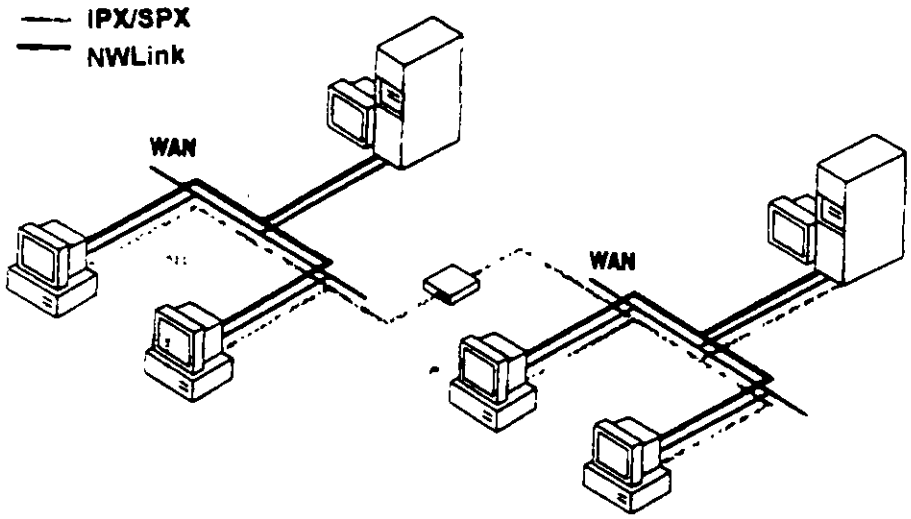
Notas:

WINDOWS NT PROTOCOLO DE RED: Net BEUI (Interfaz e[illegible]dida de u[illegible]rio NetBIOS Y TCP/IP



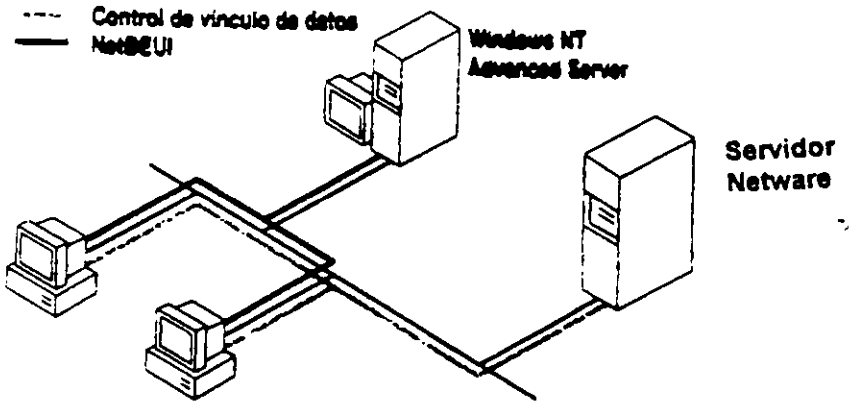
Notas:

WINDOWS NT PROTOCOLO DE RED: NWLink



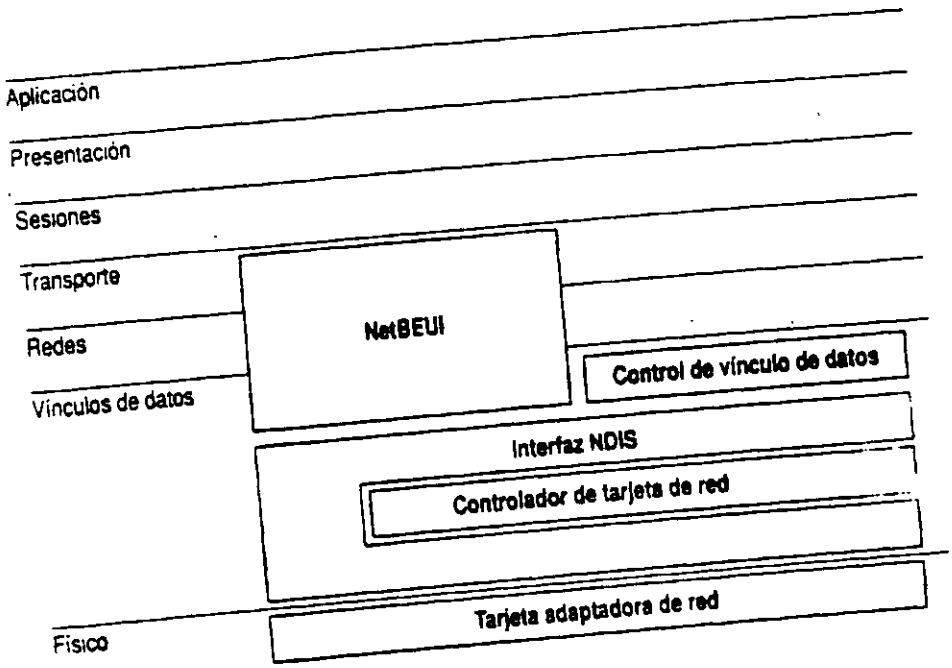
Notas:

WINDOWS NT PROTOCOLO DE RED: DLC



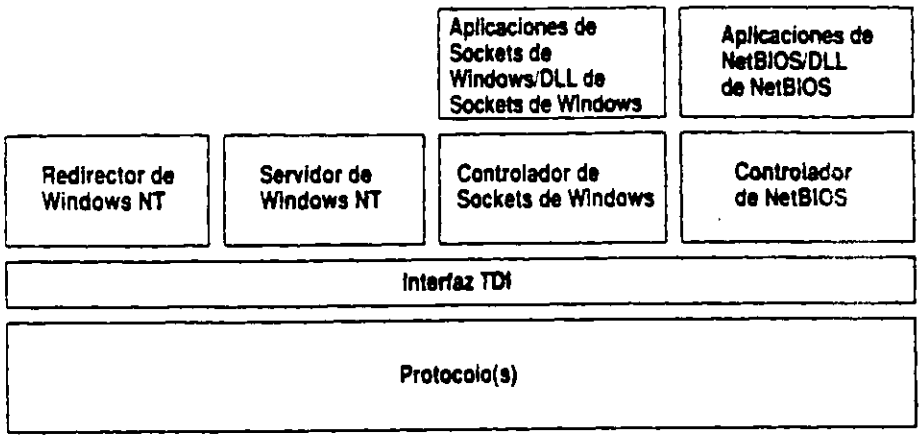
Notas:

WINDOWS NT PROTOCOLO DE RED: DLC



Notas:

WINDOWS NT INTERFAZ TDI (Interfaz de contr dor de transporte)



Notas:

INSTALACIÓN Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

3.- GRUPOS DE TRABAJO Y DOMINIOS.

Mayo de 1996.

Funcionamiento de la seguridad en la red

Windows NT Advanced Server incorpora diversos métodos de seguridad. Estos métodos proporcionan numerosas formas de controlar la actividad de los usuarios, sin por ello impedirles el acceso a los recursos que necesitan. El fundamento de la seguridad de Windows NT es que todos los recursos, y acciones están protegidos por el *control de acceso discrecional*, que significa que es posible permitir a determinados usuarios acceder a un recurso o realizar una determinada acción, y al mismo tiempo impedírselo a otros usuarios. Además, la seguridad es muy granular. Por ejemplo, es posible establecer distintos permisos sobre diferentes archivos de un mismo directorio.

Con Windows NT Advanced Server, la seguridad está integrada en el sistema operativo desde el principio, en lugar de incorporarse al mismo como un componente adicional. Esto significa que los archivos y recursos pueden protegerse incluso de los usuarios que trabajan en la misma computadora (ordenador) donde se encuentre el recurso, así como de los usuarios que accedan al recurso a través de la red. Windows NT y Windows NT Advanced Server incorporan medidas de seguridad incluso para las funciones básicas del sistema, como el propio reloj de la computadora.

Windows NT Advanced Server ofrece asimismo un modelo de administración lógico, que le ayudará a administrar de un modo eficaz una red de gran tamaño. Cada usuario sólo necesita disponer de una única cuenta, que se almacena de modo centralizado. Esta única cuenta puede proporcionar al usuario el acceso a cualquier recurso de la red, independientemente del lugar donde se encuentre. De este modo, Windows NT Advanced Server facilita a los administradores de la red la administración de las cuentas y, al mismo tiempo, simplifica el uso de la red por parte de los usuarios.

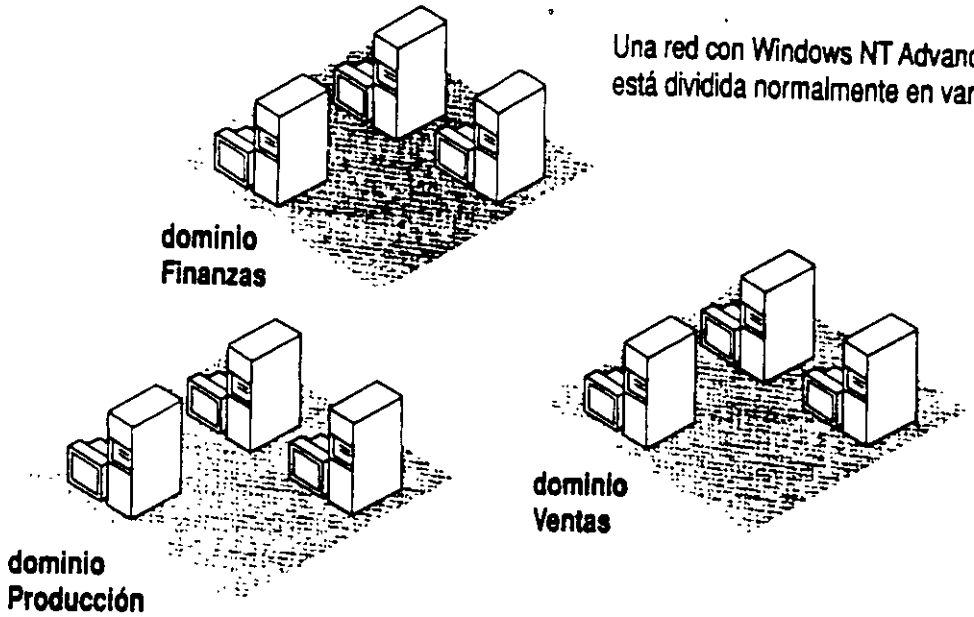
Conceptos de dominios y relaciones de confianza

La unidad básica de la administración centralizada y la seguridad en Windows NT Advanced Server es el *dominio*. Un dominio es un grupo de servidores que ejecutan Windows NT Advanced Server y, en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT Advanced Server de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que la información de una cuenta de usuario sólo necesita escribirse una vez para todos los servidores del dominio que reconocen dicha cuenta.

Las *relaciones de confianza* son vínculos entre dominios, que permiten realizar una *autentificación transparente*, en virtud de la cual un usuario sólo poseerá una cuenta de usuario en un dominio pero podrá acceder a toda la red. Si se organizan adecuadamente los dominios y relaciones de confianza de la red, todas las computadoras con Windows NT reconocerán a todas las cuentas de usuario, por lo que el usuario sólo tendrá que iniciar una sesión y facilitar una contraseña sólo una vez para acceder a cualquier servidor de la red.

Dominios: unidades administrativas básicas

La agrupación de computadoras (ordenadores) en dominios proporciona dos grandes ventajas a los usuarios y administradores de la red. Lo que es más importante, los servidores de un dominio constituyen una unidad administrativa única que comparte la información de seguridad y de cuentas de usuario. Cada dominio posee una base de datos que contiene las cuentas de los usuarios y grupos, y las configuraciones del plan de seguridad. Todos los servidores que ejecuten Windows NT Advanced Server en el dominio mantendrán una copia de esta base de datos. Ello significa que los administradores sólo necesitarán administrar una cuenta para cada usuario y que cada usuario sólo tendrá que utilizar una cuenta (y recordar una sola contraseña). Al extender la unidad administrativa desde la computadora individual hasta todo un dominio, Windows NT Advanced Server ahorra tiempo y esfuerzo tanto a los administradores como a los usuarios.



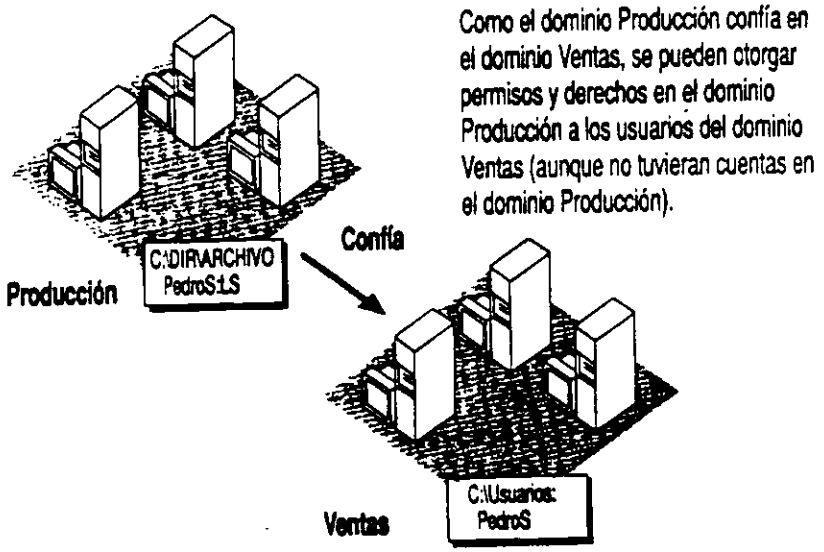
Una red con Windows NT Advanced Server está dividida normalmente en varios dominios.

La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observará que está agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo. Esta ventaja de los dominios es idéntica al concepto de *grupo de trabajo* que incorpora Windows para Trabajo en grupo. Además, los dominios de Windows NT Advanced Server son compatibles con los grupos de trabajo de Windows para Trabajo en grupo. Si desea obtener más información sobre Windows para Trabajo en grupo, consulte la sección "Interacción con computadoras (ordenadores) con Windows para Trabajo en grupo", más adelante en este mismo capítulo.

Nota No debe confundirse el concepto de dominio de Windows NT Advanced Server con los dominios del protocolo de red TCP/IP. Los dominios TCP/IP son partes de la Internet TCP/IP y no tienen nada que ver con los dominios de Windows NT Advanced Server.

Relaciones de confianza: vínculos entre dominios

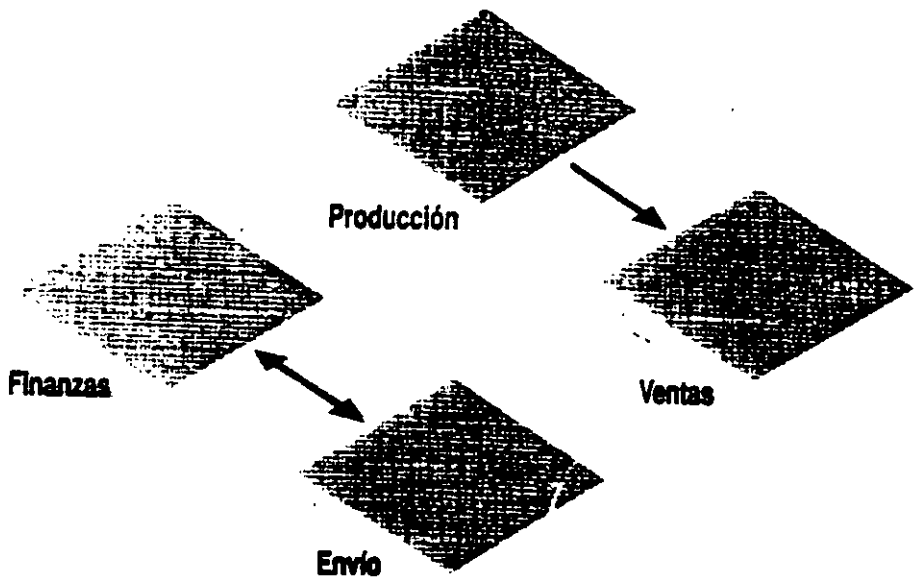
Estableciendo relaciones de confianza entre los dominios de la red, podrá permitir que determinadas cuentas de usuario y grupos globales puedan utilizarse en dominios distintos del que estén situadas dichas cuentas. (Si desea obtener más información sobre los grupos globales, consulte la sección "Utilidad de los grupos", más adelante en este mismo capítulo.) Ello facilita en gran medida la administración, ya que cada cuenta de usuario tiene que crearse una sola vez para toda la red. Además, ofrece la posibilidad de acceder a cualquier computadora (ordenador) de la red y no únicamente a las computadoras de uno de los dominios.



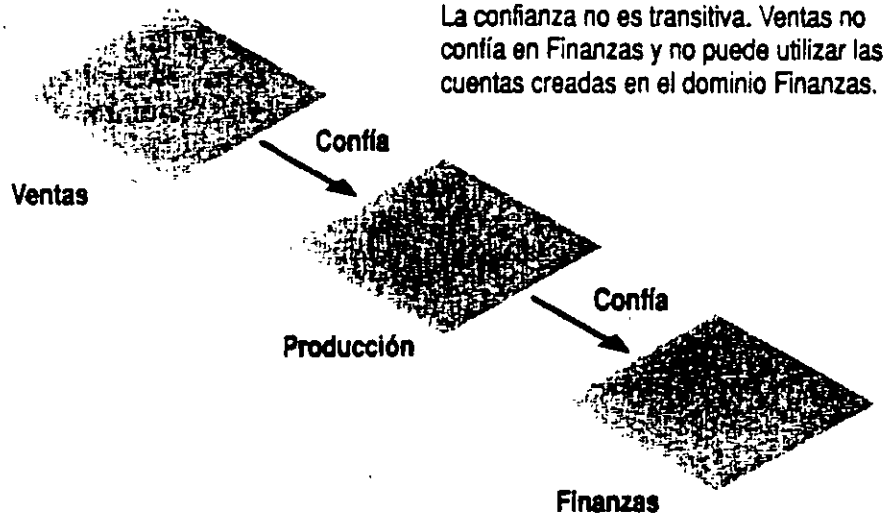
Cuando establezca una relación de confianza entre dominios, uno de los dominios (el *dominio que confía*) confiará en el otro (el *dominio en el cual se confía*).

A partir de entonces, el dominio que confía reconocerá a todos los usuarios y cuentas de grupo globales del dominio en el cual se confía. Estas cuentas podrán utilizarse como se desee dentro del dominio que confía; podrán iniciar sesiones en estaciones de trabajo situadas en el dominio que confía, integrarse en grupos locales dentro de dicho dominio, y recibir permisos y derechos dentro de ese dominio.

Las relaciones de confianza pueden ser unidireccionales o bidireccionales. Una relación de confianza bidireccional es simplemente un par de relaciones unidireccionales, en virtud del cual cada dominio confía en el otro. En la ilustración siguiente, los dominios Finanzas y Envío confían mutuamente y las cuentas de cada uno de estos dominios pueden utilizarse en el otro. Sin embargo, puesto que Producción confía en Ventas pero Ventas no confía en Producción, las cuentas de Ventas podrán utilizarse en el dominio Producción pero las cuentas de Producción no podrán emplearse en Ventas.

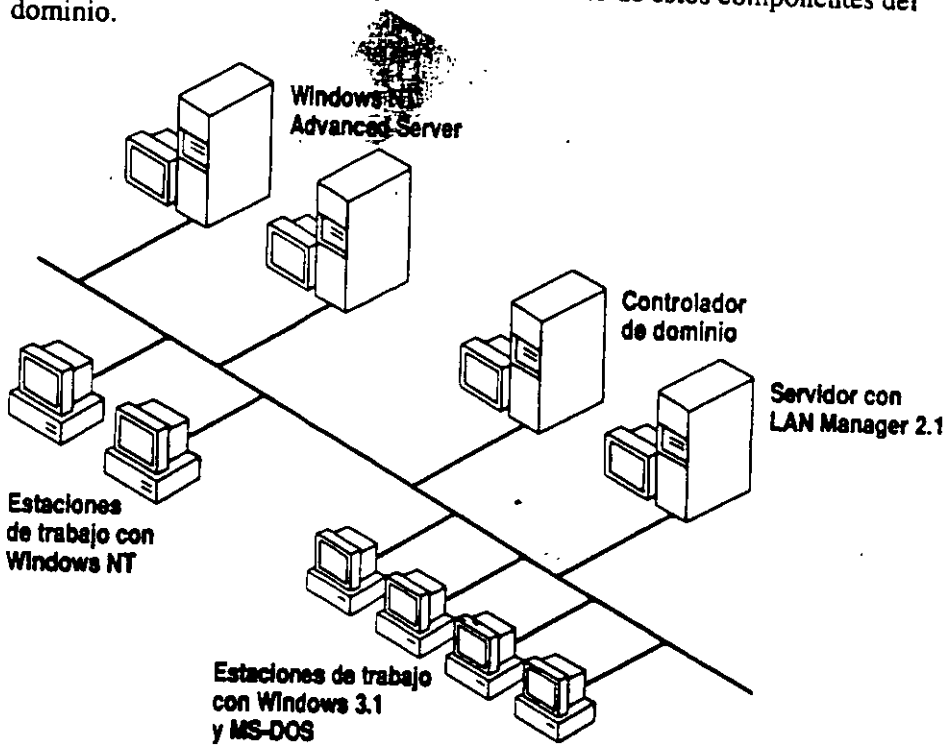


La confianza entre dominios no es una operación transitiva. Por ejemplo, si Ventas confía en Producción y Producción confía en Finanzas, Ventas no confiará automáticamente en Finanzas. Si se desea que Ventas confíe en Finanzas (para de este modo poder utilizar las cuentas de Finanzas en el dominio Ventas), deberá establecerse una relación de confianza adicional directamente entre estos dominios.



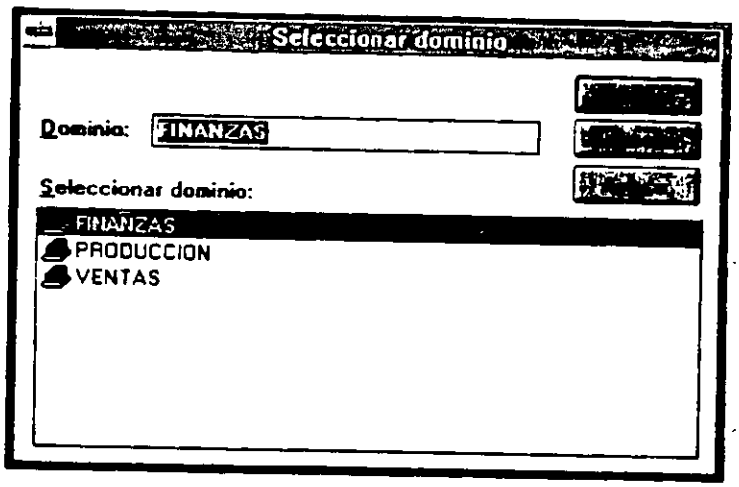
Constitución de un dominio

El requisito mínimo de un dominio es una computadora (ordenador) con Windows NT Advanced Server que actúa como *controlador de dominio*, y que almacena la copia principal de la base de datos de grupos y usuarios del dominio. Si se desea, un dominio puede incluir también otros servidores adicionales que ejecutan Windows NT Advanced Server, servidores con LAN Manager 2.x, estaciones de trabajo con Windows NT u otras estaciones de trabajo, por ejemplo aquellas que ejecutan Windows para Trabajo en grupo o MS-DOS. En las secciones siguientes se describen con mayor detalle cada uno de estos componentes del dominio.



Controlador de dominio

El controlador de dominio de un dominio que ejecuta Windows NT Advanced Server debe ser un servidor que ejecute Windows NT Advanced Server. Cualquier modificación en la base de datos de grupos y usuarios del dominio deberá realizarse en la base de datos que está almacenada en el controlador del dominio. Sin embargo, no es necesario tener que recordar el nombre de la computadora (ordenador) del controlador de dominio para cada uno de los dominios. Cuando utilice el Administrador de usuarios de dominios para modificar la base de datos de usuarios, sólo necesitará conocer el nombre del dominio en el cual desee realizar los cambios. El cambio se realizará automáticamente en el controlador del dominio. El Administrador de usuarios para dominios no permite modificar directamente la base de datos de usuarios de un servidor del dominio que no sea el controlador de dominio.



Otros servidores

Otros servidores del dominio que ejecuten Windows NT Advanced Server almacenarán también copias de la base de datos de cuentas del dominio.

La base de datos de cuentas del dominio estará duplicada en cada uno de los servidores del dominio que ejecuten Windows NT Advanced Server. Los otros servidores del dominio consultarán al controlador del dominio cada 5 minutos, preguntándole si se ha realizado algún cambio en la base de datos. Si en este período de 5 minutos se ha realizado alguna modificación, el controlador del dominio enviará dichos cambios a los otros servidores (sólo se enviarán los cambios; no será necesario copiar toda la base de datos).

Todos los archivos del dominio que ejecuten Windows NT Advanced Server podrán procesar las peticiones de inicio de sesión por parte de las cuentas de usuario del dominio. Cuando el dominio reciba una petición de inicio de sesión, cualquiera de los servidores del dominio podrá autentificar el intento de inicio de sesión. (Por tanto, todos los servidores del dominio actuarán igual que los controladores de seguridad de dominios de reserva en LAN Manager 2.x.)

Es muy recomendable que, además del controlador de dominio, uno o varios servidores del dominio estén ejecutando Windows NT Advanced Server. Estos servidores adicionales proporcionan un mecanismo de seguridad: si el controlador de dominio no está disponible, cualquier otro servidor podrá ser promovido al puesto de controlador de dominio, lo cual permitirá al dominio seguir funcionando. La existencia de varios servidores permite también distribuir la carga de trabajo relacionada con las peticiones de inicio de sesión, lo cual resulta especialmente útil en dominios con un gran número de cuentas de usuario.

Servidores con LAN Manager 2.x

Los servidores con LAN Manager 2.x pueden actuar como servidores dentro de un dominio cuyo controlador ejecute Windows NT Advanced Server. Sin embargo, un servidor con LAN Manager 2.x no puede ser controlador de dominio dentro de un dominio que ejecuta Windows NT Advanced Server, ya que LAN Manager 2.x no incorpora todos los tipos de información que contienen las cuentas de Windows NT Advanced Server.

Los servidores con LAN Manager 2.x almacenarán una copia de la base de datos de cuentas de usuarios del dominio. Podrán validar los intentos de inicio de sesión que se realicen desde estaciones de trabajo con Windows para Trabajo en grupo o LAN Manager 2.x, pero no podrán validar los inicios de sesión de los usuarios de Windows NT. No es aconsejable recurrir únicamente a servidores con LAN Manager 2.x como servidores de reserva dentro de un dominio que ejecuta Windows NT Advanced Server, ya que no pueden autentificar las peticiones de inicio de sesión desde estaciones de trabajo con Windows NT y no podrán ser promovidos a controladores de dominio dentro de un dominio que ejeucta Windows NT Advanced Server.

Si desea obtener más información sobre el empleo de servidores con LAN Manager 2.x en la red, consulte la sección "Interacción con servidores ejecutando otros sistemas de red", más adelante en este mismo capítulo.

Estaciones de trabajo con Windows NT

Para cada una de las estaciones de trabajo con Windows NT de la red, podrá optar entre integrar la estación de trabajo en un dominio o en un grupo de trabajo. En la mayoría de los casos, lo más conveniente será integrar cada una de las estaciones de trabajo con Windows NT en un dominio. Este es el único modo de que un usuario con cuenta en un dominio que ejecuta Windows NT Advanced Server pueda iniciar una sesión con esa cuenta en una estación de trabajo con Windows NT.

Una estación de trabajo con Windows NT que forme parte de un dominio no obtendrá en realidad una copia de la base de datos de usuarios del dominio. Sin embargo, podrá aprovechar las ventajas que ofrece la base de datos de grupos y usuarios del dominio. Para obtener más información al respecto, consulte la sección "Interacción con estaciones de trabajo con Windows NT", más adelante en este mismo capítulo.

Una estación de trabajo con Windows NT perteneciente a un grupo de trabajo dispondrá de su propia base de datos de usuario y procesará personalmente las peticiones de inicio de sesión. Ninguna de las computadoras (ordenadores) de un grupo de trabajo comparte información sobre cuentas. En este tipo de estaciones de trabajo, sólo será posible iniciar sesiones o recibir derechos o permisos para la estación de trabajo cuando se utilicen cuentas de usuario que hayan sido creadas en la propia estación de trabajo.

Si desea obtener más información sobre los dominios y grupos de trabajo, consulte la sección "Interacción con computadoras con Windows para Trabajo en grupo", más adelante en este mismo capítulo.

Estaciones de trabajo con MS-DOS

Las estaciones de trabajo con MS-DOS no pueden almacenar cuentas de usuario, por lo que no es necesario que pertenezcan a dominios como sucede con las computadoras con Windows NT. Normalmente, cada estación de trabajo con MS-DOS dispondrá de un conjunto de dominios predeterminado para examinar la red. Si un usuario de una estación de trabajo con MS-DOS posee una cuenta en el dominio, podrá configurarse como dominio examinador en la estación de trabajo del usuario en cualquier dominio; no es necesario que sea el dominio que contiene la cuenta del usuario.

Modelos de dominios

El método que se utilice para planificar y organizar los dominios de una red es decisivo. Si se configuran los dominios de tal modo que todas las cuentas de usuario y grupos globales sean válidos en todos los dominios, podrá simplificarse extraordinariamente la administración de la red, garantizando al mismo tiempo que todos los usuarios puedan acceder a la totalidad de la misma.

Existen cuatro modelos de organización de la red que permiten obtener este objetivo: el *modelo de dominio único*, el *modelo de dominio maestro*, el *modelo de dominio maestro múltiple* y el *modelo de confianza total*. En las secciones siguientes se describen estos cuatro modelos. Puede optar por seguir fielmente uno de estos modelos, modificar alguno o combinarlos entre sí en las distintas partes de la red.

Las figuras que aparecen en las secciones siguientes hacen referencia a grupos locales y grupos globales. Si desea obtener más información en este sentido, consulte la sección "Utilidad de los grupos" que aparece más adelante en este mismo capítulo.

Modelo de dominio único

Si su red no tiene demasiados usuarios y no necesita dividirla con fines organizativos, puede utilizar el modelo de dominio más sencillo, o sea el modelo de dominio único. Con este modelo, la red estará formada por un solo dominio. Naturalmente, todos los usuarios y grupos globales serán creados en ese dominio. No será necesario establecer relaciones de confianza, ya que sólo existirá un dominio en toda la red.

Una red podrá utilizar el modelo de dominio único si no tiene más de 10.000 usuarios y grupos aproximadamente (el número exacto dependerá de la velocidad del procesador y de la cantidad de memoria RAM de los servidores del dominio).

Si en su red hay muchos servidores que comparten recursos o si su organización está dividida en numerosos departamentos, puede que el modelo de dominio único no sea el más adecuado. Con dominios múltiples, cuando un usuario examine la red, observará primero cuáles son los dominios existentes, escogerá uno de ellos y examinará los recursos que contiene. Si su red integra numerosos recursos compartidos, dividiéndola en dominios facilitará la búsqueda de los recursos. Además. la consulta de dominios únicos con muchos servidores resulta más lenta para los usuarios.

Además, la existencia de un solo dominio significa que los administradores de la red podrán administrar en cualquier momento todos los servidores de la misma, ya que la facultad de administrar servidores está asociada al nivel de dominio. Dividiendo una red en varios dominios podrá establecer varios administradores que puedan administrar únicamente determinados servidores, por ejemplo, los de sus propios departamentos.

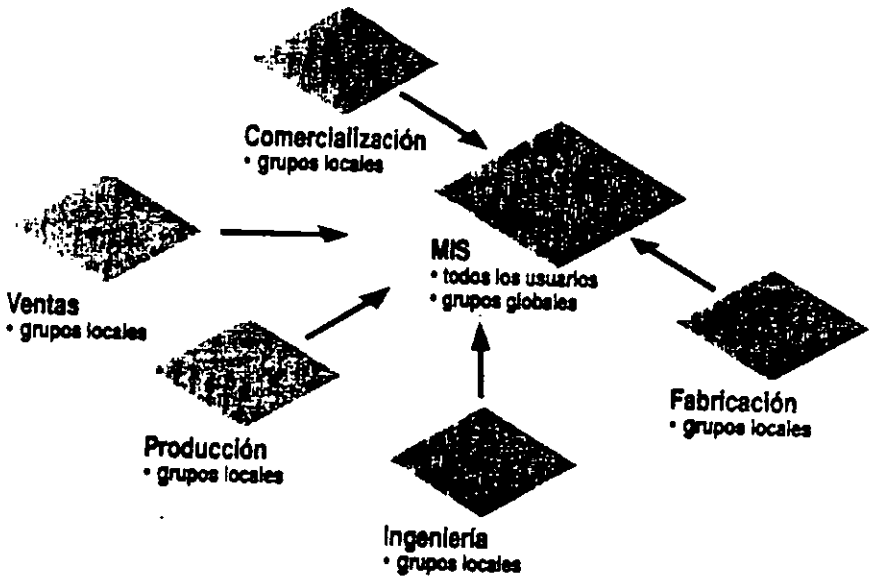
La siguiente tabla muestra las ventajas y desventajas de la utilización del modelo de dominio único.

Ventajas	Desventajas
Es el más indicado para empresas con pocos usuarios y recursos.	No puede utilizarse en empresas que tengan más de 10.000 usuarios.
Administración centralizada de las cuentas de usuario.	No permite agrupar los usuarios en departamentos.
No es necesario administrar relaciones de confianza.	No permite agrupar recursos.
Los grupos locales sólo tienen que definirse una vez.	El examen de la red resulta más lento si el dominio incorpora un gran número de servidores.

Modelo de dominio maestro

El modelo de dominio maestro será probablemente la opción más adecuada para aquellas compañías en las cuales sea necesario dividir la red en varios dominios con fines organizativos, pero cuya red no tenga más de 10.000 usuarios y grupos. Este modelo proporciona las ventajas de organización y administración centralizada que poseen dominios múltiples.

Con este modelo, existirá un dominio (el *dominio maestro)* en el cual se crearán todos los usuarios y grupos globales de la red. Los demás dominios de la red confiarán en este dominio y, por lo tanto, podrán utilizar los usuarios y grupos globales definidos en él. Si su empresa posee un departamento de administración de sistema de información (MIS) que se encargue de administrar la red local, lo lógico será que dicho departamento sea el que administre el dominio maestro.



Un dominio maestro puede considerarse como un dominio de cuentas, cuyo propósito principal es administrar las cuentas de usuario de la red. Los demás dominios de la red serán dominios de recursos, ya que en ellos no se almacenará ni administrará ninguna cuenta de usuario, sino que su única finalidad será proporcionar recursos (como impresoras y archivos compartidos) a la red.

Con este modelo, únicamente los servidores del dominio maestro tendrán copias físicas de la base de datos de cuentas de la red. Conviene asegurarse de disponer al menos de un servidor adicional que ejecute Windows NT Advanced Server en el dominio maestro, para que, en caso de fallo del controlador de dominio, dicho servidor adicional pueda asumir el control y permitir que la red siga funcionando.

La siguiente tabla muestra las ventajas y desventajas de la utilización del modelo de dominio maestro.

Ventajas	Desventajas
Es la opción más indicada para empresas que tengan menos de 10.000 usuarios y necesiten que los recursos compartidos se dividan en grupos.	No puede utilizarse en empresas con más de 10.000 usuarios.
Permite administrar las cuentas de usuario de manera centralizada.	Obliga a definir grupos locales en cada uno de los dominios donde vayan a utilizarse.
Los recursos se agrupan de una manera lógica.	
Los dominios de los distintos departamentos pueden tener sus propios administradores, que se encargarán de controlar los recursos del departamento.	
Sólo es necesario definir los grupos globales una vez (en el dominio maestro).	

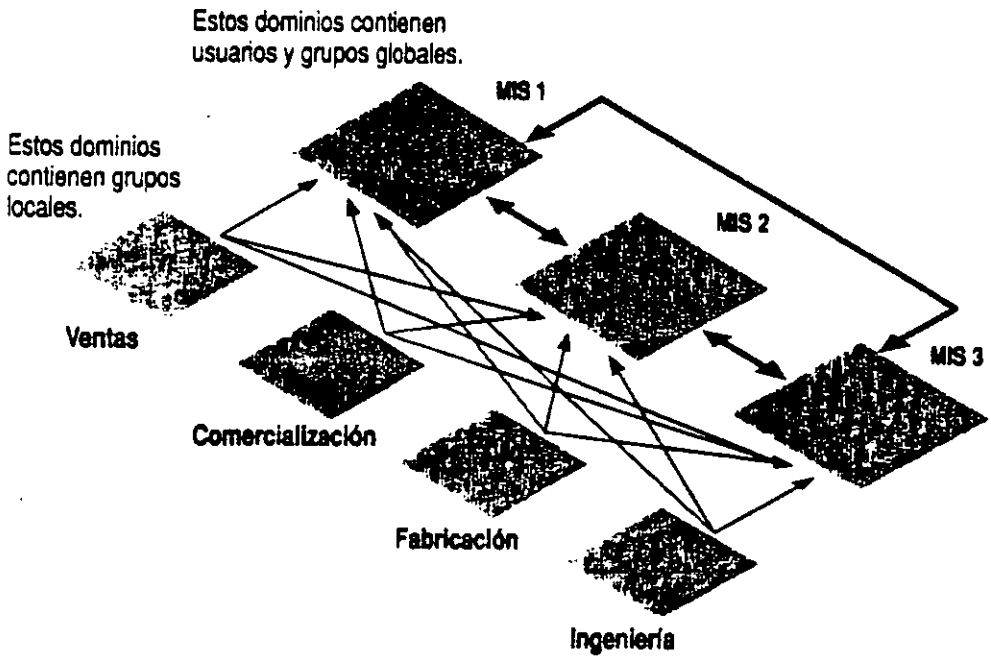
Existe una variante de este modelo que puede utilizarse en empresas en las cuales existan varias divisiones diferentes, cada una de ellas con su propia administración de sistema de información (MIS). En este caso, las distintas divisiones tendrían sus respectivos dominios maestros, cada uno de los cuales englobaría a los usuarios que trabajen en la división respectiva. Cada uno de los dominios departamentales confiará probablemente en un solo dominio maestro: el dominio maestro de la división a la cual pertenezca dicho departamento. Sin embargo, si un dominio departamental lo necesita, podrá confiar en más de un dominio maestro. Los dominios maestros probablemente no necesitarán confiar entre sí.

Modelo de dominio maestro múltiple

En empresas de gran tamaño que deseen disponer de administración centralizada, el modelo de dominio maestro múltiple puede ser la opción más indicada, ya que es el que ofrece mayores posibilidades de ampliación.

En este modelo existe un número reducido de dominios maestros. Los dominios maestros actúan como dominios de cuentas. Toda cuenta de usuario de la red será creada en alguno de estos dominios maestros. La administración de sistema de información (MIS) de la empresa podrá administrar los dominios maestros. Aparte de los dominios maestros, existirán otros, los dominios departamentales, que proporcionarán recursos. Los dominios departamentales podrán ser administrados por los miembros del departamento respectivo o bien, por el departamento de MIS.

Cada uno de los dominios maestros confía en todos los demás dominios maestros. Cada uno de los dominios departamentales confía en todos los dominios maestros, pero los dominios departamentales no necesitan confiar entre sí.



Puesto que cualquier cuenta de usuario de la empresa existe en alguno de los dominios maestros y todos los dominios de la empresa confían en todos los dominios maestros, cualquier cuenta de usuario de la empresa podrá utilizarse en cualquiera de los dominios.

Obsérvese que con este modelo resulta algo más difícil utilizar grupos globales. Si se necesita que un grupo global incluya usuarios procedentes de dos o más de los dominios maestros, en realidad será necesario crear varios grupos globales (uno para cada dominio maestro) y utilizar todos estos grupos globales, cuando en otros modelos de dominios sólo se utilizaría un grupo global.

Para reducir al mínimo el problema de los grupos globales, conviene distribuir los usuarios entre los distintos dominios maestros clasificándolos por organizaciones dentro de la empresa, en lugar de ordenarlos alfabéticamente o por algún otro método. De este modo, se reducirá la posibilidad de que sea necesario establecer grupos globales similares desde dominios maestros diferentes. (Si desea una explicación sobre los grupos globales, consulte la sección "Diferencias entre los grupos globales y locales", más adelante en este mismo capítulo.)

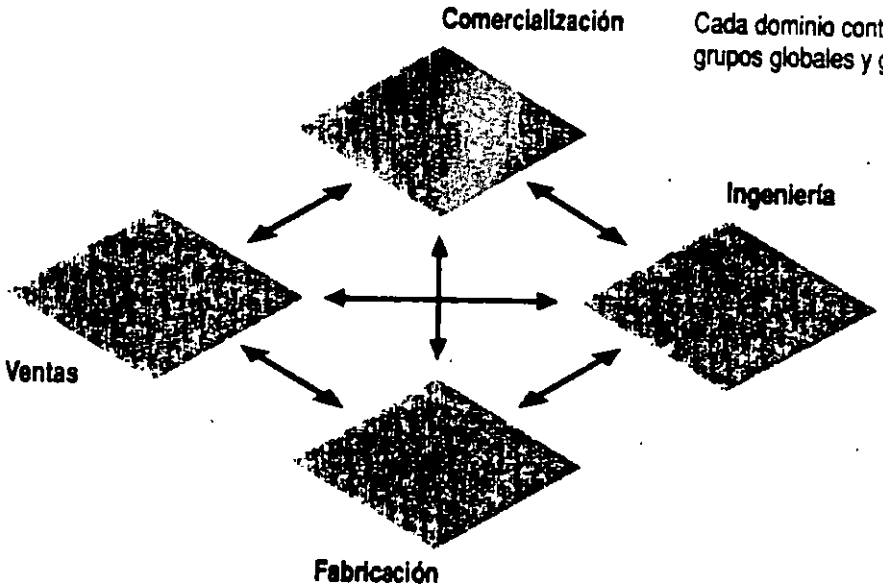
Todos los dominios maestros podrán ser administrados por el departamento central de MIS de la empresa.

La siguiente tabla muestra las ventajas y desventajas de la utilización del modelo de dominio maestro múltiple.

Ventajas	Desventajas
Es la opción más indicada para empresas con 10.000 usuarios o más, y con departamento de MIS centralizado.	Puede ser necesario definir varias veces tanto los grupos locales como los globales.
Puede ampliarse hasta obtener redes con cualquier número de usuarios.	Obliga a administrar un mayor número de relaciones de confianza.
Los recursos están agrupados de una forma lógica.	No todas las cuentas de usuario están situadas en el mismo dominio.
Los dominios departamentales pueden tener sus propios administradores, responsables de administrar los recursos de sus respectivos departamentos.	

Modelo de confianza total

Si desea que la administración de los usuarios y dominios quede distribuida entre los distintos departamentos, en lugar de centralizarla, puede que prefiera utilizar el modelo de confianza total. Con este modelo, todos los dominios de la red confiarán en todos los demás dominios. De este modo, cada departamento podrá administrar su propio dominio y definir sus propios usuarios y grupos globales, los cuales podrán utilizarse también desde los demás dominios de la red.



El gran número de relaciones de confianza que obliga a establecer este modelo hace que no resulte práctico para empresas de gran tamaño. Con el modelo de confianza total, el número de relaciones de confianza que haría falta establecer para una empresa con n dominios es *n*(n-1)*. Por ejemplo, para 10 dominios serían necesarias 90 relaciones de confianza y para 20 dominios serían necesarias 380. La incorporación de un nuevo dominio a una red existente de 10 dominios obligaría a establecer 20 nuevas relaciones de confianza.

Pese a estas cifras, este modelo puede ser el mejor para aquellas empresas que no posean departamentos de MIS centralizados o para los departamentos pertenecientes a empresas que no hayan establecido Windows NT Advanced Server como estándar general.

Con este modelo se hace más patente la idea del término "confianza". Antes de crear una relación de confianza con otro dominio, deberá estar seguro de que confía en el administrador de dicho dominio, especialmente si va a otorgar permisos de acceso a sus grupos globales para los usuarios de aquel dominio. Una vez haya concedido un permiso a un grupo local desde otro dominio (o haya incluido el grupo global en un grupo local de su dominio), estará confiando en que el administrador del otro dominio no va a incorporar a ese grupo global ningún usuario no autorizado o inadecuado en el futuro. La siguiente tabla muestra las ventajas y desventajas de la utilización del modelo de dominio de confianza total.

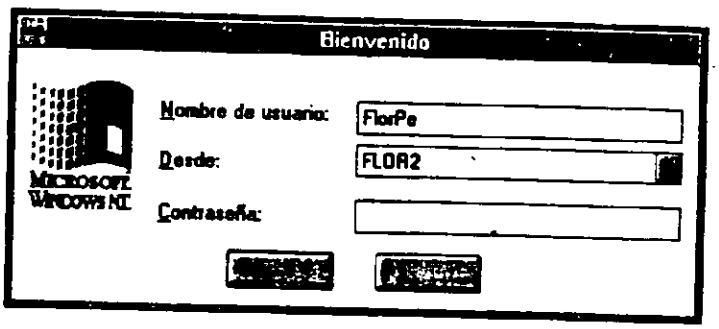
Ventajas	Desventajas
Es el más adecuado para empresas sin departamento de MIS.	Puesto que no existe una administración de usuarios centralizada, este modelo no resulta práctico para empresas que cuenten con departamentos de MIS centralizados.
Puede ampliarse hasta configurar redes con cualquier número de usuarios.	Obliga a administrar un gran número de relaciones de confianza.
Cada departamento tiene un control absoluto sobre sus recursos y cuentas de usuario.	Cada departamento debe confiar en que los otros departamentos no van a agregar usuarios inadecuados a sus grupos globales.
Tanto los recursos como las cuentas de usuario quedan agrupados en unidades departamentales.	

Autentificación de los inicios de sesión

En esta sección se describe el proceso de autentificación de los intentos de inicio de sesión realizados desde estaciones de trabajo con Windows NT, Windows 3.1 o MS-DOS.

Inicio de sesión desde una estación de trabajo con Windows NT

Cada vez que un usuario inicie una sesión en una estación de trabajo con Windows NT (escribiendo la información correspondiente en la pantalla de inicio de sesión que se muestra en la siguiente figura), se le pedirá que escriba un nombre de usuario, una contraseña y un dominio.



El nombre de usuario y la contraseña son autoexplicativos. Lo que el usuario deberá seleccionar en el cuadro "Desde" dependerá del lugar donde se encuentre su cuenta de usuario. Si dicha cuenta está en un dominio con Windows NT Advanced Server, el usuario seleccionará ese dominio. A continuación, la estación de trabajo enviará el nombre de usuario y la contraseña al dominio especificado para su autentificación. Un servidor de ese dominio verificará el nombre de usuario y la contraseña con la base de datos de usuarios del dominio. Si el nombre de usuario y la contraseña coinciden con alguna de las cuentas, el servidor comunicará a la estación de trabajo que el inicio de sesión está autorizado. El servidor transferirá asimismo la información de inicio de sesión del usuario, por ejemplo su perfil, su directorio base y sus variables de entorno. Si desea obtener más información al respecto, consulte el capítulo 4, "Administración de entornos de usuario".

Si el usuario está iniciando una sesión en una cuenta almacenada localmente en la misma estación de trabajo, en el cuadro "Desde" deberá seleccionar el nombre de la estación de trabajo, en lugar del nombre de un dominio. Luego, la estación de trabajo verificará el nombre de usuario y la contraseña especificados por el usuario con su propia base de datos. Si los encuentra en su base de datos, autorizará el inicio de sesión y proporcionará la información de inicio de sesión del usuario, a partir de la cuenta existente en esa estación de trabajo.

Inicio de sesión desde un servidor con Windows NT Advanced Server

El proceso de inicio de sesión en una computadora (ordenador) con Windows NT Advanced Server es idéntico al utilizado en una estación de trabajo con Windows NT, excepto en dos detalles:

- Los servidores no mantienen cuentas locales distintas de las cuentas del dominio que contiene el servidor. Por tanto, el usuario deberá iniciar la sesión en una cuenta de dominio.
- El cuadro "Desde" del cuadro de diálogo **Bienvenido** será "Dominio", en lugar de "Desde".

Obsérvese que, como opción predeterminada, no se permite a cualquiera que tenga cuenta en un dominio el inicio de una sesión local desde un servidor del dominio. Sólo se permitirá hacerlo a los miembros de los grupos Administradores, Operadores de servidores, Operadores de impresión, Operadores de cuentas y Operadores de copia de seguridad. Si desea obtener más información al respecto, consulte las secciones "Distintos tipos de usuarios" y "Control de las facultades de los usuarios", más adelante en este mismo capítulo.

Inicio de una sesión desde una estación de trabajo con MS-DOS

Las estaciones de trabajo con MS-DOS no son seguras. No existe ninguna forma de impedir que un usuario no autorizado envíe peticiones de acceso a la red desde una estación de trabajo con MS-DOS. Sin embargo, sí es posible impedir que un usuario no autorizado de MS-DOS obtenga acceso a los recursos de la red. Para ello bastará con proteger los propios recursos, de tal modo que las peticiones que realice el usuario a través de la red no consigan su propósito, en caso de que dicho usuario no esté autorizado.

Si un usuario con cuenta en un dominio con Windows NT Advanced Server posee una estación de trabajo con MS-DOS, no se comprobará su identidad en el momento de iniciar la sesión (aun cuando el usuario introduzca un nombre de usuario y una contraseña). Sin embargo, el nombre de usuario y la contraseña se verificarán la primera vez que dicho usuario acceda a un servidor con Windows NT. El servidor comprobará si el nombre de usuario y la contraseña coinciden con los de alguna de las cuentas del dominio de ese servidor (o de algún dominio de confianza del dominio al cual pertenezca el servidor). De este modo, los usuarios de estaciones de trabajo con MS-DOS podrán disponer de cuentas de dominio y estar sujetos a autorizaciones sobre sus cuentas.

Conceptos de usuarios y grupos

Cualquier persona que utilice la red con regularidad debe disponer de una *cuenta de usuario* en algún dominio de la misma. La cuenta de usuario contiene datos diversos sobre el usuario, como su nombre, contraseña y limitaciones de uso de la red. También es posible agrupar usuarios con trabajos o necesidades de recursos similares dentro de *grupos globales* y *grupos locales*; los grupos simplifican la concesión de derechos y permisos de uso de recursos, ya que basta con conceder a un grupo un determinado derecho o permiso, para que tal derecho o permiso quede concedido automáticamente a todos los miembros presentes y futuros de ese grupo.

Asimismo, las cuentas de usuario están subdivididas en dos tipos: *cuentas de usuario globales* y *cuentas de usuario locales*. La mayoría de las cuentas de usuario que cree serán cuentas de usuario globales. Si desea obtener más información sobre las cuentas de usuario locales, consulte la sección "Concepto de cuenta local", más adelante en este mismo capítulo.

Las cuentas de usuario y de grupo son creadas y administradas por el Administrador de usuarios. El Administrador de archivos se utiliza para conceder a los usuarios y grupos permisos sobre archivos y directorios. El Administrador de impresión se utiliza para conceder acceso a las impresoras. Si desea obtener más información sobre estos temas, consulte el capítulo 5, "Administración de archivos de la red" y el capítulo 6, "Uso compartido de impresoras".

Contenido de una cuenta de usuario

En la tabla siguiente se muestra el contenido de cada una de las cuentas de usuario.

Elemento de la cuenta	Comentario
Nombre de usuario	Nombre exclusivo que el usuario escribirá cuando inicie una sesión. Suele estar formado por una combinación de partes del primer nombre y apellido del usuario.
Contraseña	Contraseña secreta del usuario.
Nombre completo	Nombre completo del usuario.
Horas de inicio de sesión	Horas durante las cuales el usuario podrá iniciar sesiones. Este dato afecta tanto a su posibilidad de iniciar una sesión en la red como acceder a los servidores. En el plan de seguridad del dominio es posible especificar si se obligará a los usuarios a desconectarse o cerrar la sesión cuando termine el período durante el cual están autorizados a conectarse. Si desea obtener más información al respecto, consulte la sección "Configuración del plan de cuentas y contraseñas", más adelante en este mismo capítulo.
Estaciones de trabajo para inicio de sesión	Nombres de las estaciones de trabajo desde las cuales el usuario está autorizado a trabajar. Como opción predeterminada, el usuario podrá emplear cualquier estación de trabajo, aunque, si se desea, es posible establecer limitaciones en este sentido.
Fecha de caducidad	Fecha futura en la cual la cuenta será desactivada automáticamente. Resulta útil para garantizar que las cuentas de estudiantes o empleados temporales no se mantengan activas innecesariamente.
Directorio base	Directorio del servidor que pertenecerá privadamente al usuario, el cual podrá controlar el acceso al mismo.
Archivo de comandos de inicio de sesión	Archivo por lotes o archivo ejecutable que se ejecutará automáticamente cuando el usuario inicie una sesión.
Perfil	Archivo que contiene un registro del entorno o del escritorio del usuario, con información como los grupos de programa, las conexiones de red y los colores de pantalla, así como las opciones que determinan los aspectos del entorno que el usuario podrá cambiar. Si desea obtener más información sobre los perfiles de usuario, consulte el capítulo 4, "Administración de entornos de usuario".
Tipo de cuenta	El tipo de cuenta puede ser global o local. La mayoría de las cuentas que cree serán globales. Si desea obtener más información sobre las cuentas, consulte la sección "Concepto de cuenta local", más adelante en este mismo capítulo. Esta opción sólo está disponible en dominios de Windows NT Advanced Server.

Asimismo, existen varias condiciones que se cumplirán o no para cada una de las cuentas de usuario, como se muestra en la tabla siguiente.

Condición de la cuenta	Predeterminado	Comentarios
¿Cambiar la contraseña en el siguiente inicio de sesión?	Sí	Si esta opción está seleccionada, se obligará al usuario a cambiar la contraseña la próxima vez que inicie una sesión, momento en el cual este valor será sustituido por No.
El usuario no puede cambiar la contraseña	No	Si este valor es afirmativo, el usuario no podrá cambiar su propia contraseña. Esta opción resulta útil para cuentas compartidas.
La contraseña nunca caduca	No	Si la respuesta es afirmativa, para esta cuenta de usuario se ignorará la política de caducidad de contraseñas que haya sido establecida para ese dominio, con lo cual la contraseña nunca caducará. Esta opción resulta útil para cuentas que representen servicios, como el servicio Duplicador. También es útil para cuentas a las cuales no se desee cambiar nunca la contraseña, como por ejemplo, las cuentas Invitado.
Cuenta desactivada	No	Si la respuesta es afirmativa, esta cuenta será desactivada y no podrá iniciarse una sesión con ella. No se eliminará de la base de datos, pero nadie podrá iniciar una sección con ella hasta que no se active de nuevo. Esta opción es útil para las cuentas que se usen como plantilla.

Cada cuenta de usuario tiene asociado además un identificador de seguridad (SID), es decir, un número exclusivo que la identifica de forma unívoca. Toda cuenta que haya sido creada alguna vez en su red tendrá un SID distinto del de cualquier otra. Los procesos internos de Windows NT no hacen referencia al nombre de usuario de una cuenta, sino al número SID de la misma. Por lo tanto, si se crea una cuenta, si se elimina dicha cuenta y si posteriormente se crea otra nueva con el mismo nombre de usuario, la nueva cuenta no adquirirá ninguno de los derechos o permisos que hubieran sido concedidos a la cuenta anterior, ya que ambas tendrán números SID diferentes.

En algunas pantallas de Windows NT Advanced Server, por ejemplo, en el Administrador de usuarios de dominios y en el Administrador de archivos, los nombres de usuario pueden aparecer precedidos por el dominio donde reside la cuenta de usuario. Esto sucederá únicamente cuando se examinen cuentas situadas en dominios distintos del dominio de observación actual. Ello proporciona más información sobre los usuarios examinados y, además, permite identificarlos de una manera precisa. Por ejemplo, el usuario JuanL del dominio Ventas aparecería como Ventas\JuanL. Podrían existir varios usuarios JuanL en dos dominios, pero no habría lugar a confusión, puesto que Windows NT Advanced Server los mostraría como Ventas\JuanL e Ingeniería\JuanL.

Nota Las cuentas de usuario pueden contener una gran cantidad de información. En una red de gran tamaño, escribir toda esa información para cada usuario puede exigir demasiado tiempo, pero con Windows NT Advanced Server existen varios métodos que facilitan la creación de cuentas de usuario. Una nueva cuenta puede crearse copiando otra cuenta existente y cambiando únicamente el nombre de usuario y la contraseña inicial, así como cualquier otra información que deba modificarse. Ello permite también crear una o varias *cuentas plantilla*, es decir, cuentas que no sean utilizadas por usuarios reales, sino que sirvan únicamente como base para crear cuentas reales. Para mayor seguridad, es posible desactivar las cuentas utilizadas como plantilla, para garantizar que ningún usuario pueda iniciar una sesión con ellas.

Utilidad de los grupos

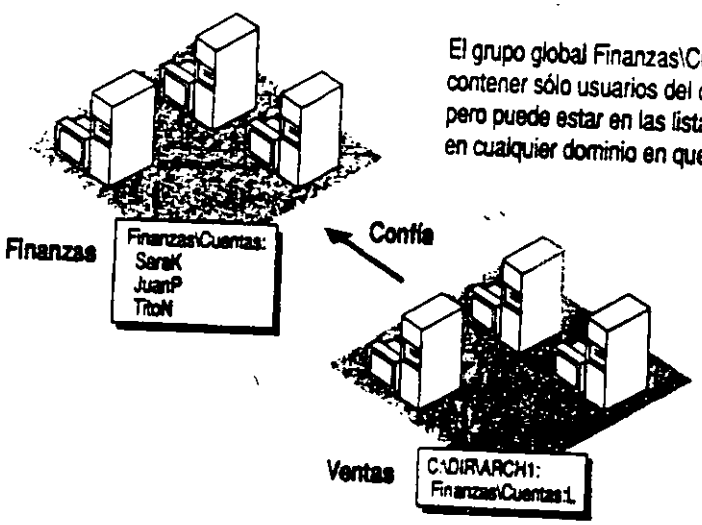
La inte[illegible]ción de usuarios en grupos permite conceder a varios usuarios el acceso a un rec[illegible] de una forma más fácil y rápida. Para conceder un permiso o derecho a todos los usuarios de un grupo, bastará con otorgar tal derecho o permiso al propio grupo. Otra ventaja de los grupos es cuando algún nuevo usuario se afilia a la red. Por ejemplo, si se contrata a un nuevo contable y existe un grupo Contables que posee los permisos que necesitan los contables, bastará con incorporar al nuevo usuario al grupo Contables para otorgarle todos los permisos que pueda necesitar en una sola operación.

En un dominio con Windows NT Advanced Server o en una estación de trabajo con Windows NT, los grupos locales ofrecen además un método para clasificar usuarios y asignarles rápidamente conjuntos predefinidos de derechos y permisos. Por ejemplo, para convertir a una cuenta en operador de impresión de un dominio, bastará con incorporar dicha cuenta al grupo local "Operadores de impresión" del dominio. Con ello, la cuenta adquirirá todos los derechos y facultades de un operador de impresión.

Funcionamiento de los grupos globales

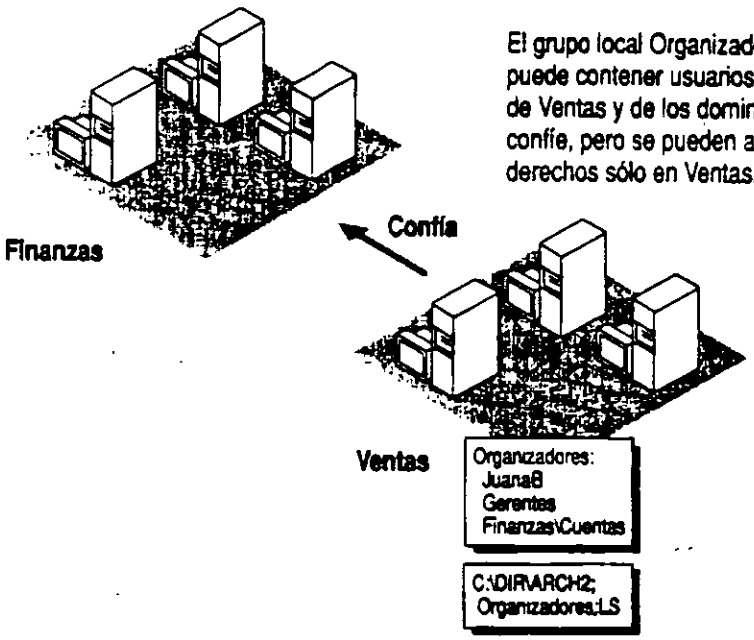
Un *grupo global* es un conjunto de cuentas de usuario de un dominio que se reúnen bajo un mismo nombre de grupo. Un grupo global sólo puede contener cuentas de usuario del dominio en el cual haya sido creado. Una vez creado un grupo global, podrá estar disponible desde cualquier punto. Podrá recibir permisos y derechos en su propio dominio y en cualquiera de los dominios que confíen en el suyo. Un grupo global sólo puede contener cuentas de usuario; no puede incluir otros grupos locales o globales.

En algunas pantallas de *Windows NT Advanced Server* observará que el nombre de un grupo global aparece precedido por el nombre del dominio donde reside. Por ejemplo, cuando examine los permisos de archivo de un servidor perteneciente al dominio Ventas, si los usuarios pertenecientes al grupo global Directores del dominio Finanzas poseen permisos, aparecerán como Finanzas\Directores. De este modo, cada grupo global dispondrá de una identificación absoluta cuando se haga referencia a él desde cualquier dominio distinto del suyo propio. (Cuando un grupo global sea examinado dentro de su propio dominio, no aparecerá como prefijo el nombre del dominio; por ejemplo, cuando examine permisos de archivo en un servidor perteneciente al dominio Ventas, los grupos globales situados en el propio dominio Ventas se identificarán únicamente con el nombre del grupo.)



Funcionamiento de los grupos locales

Un *grupo local* es un conjunto de usuarios y grupos globales procedentes de uno o varios dominios, que se reúnen bajo un solo nombre de grupo. Aunque un grupo local de un dominio podrá contener usuarios y grupos globales de ese dominio, así como de cualquier otro de su confianza, sólo está permitido conceder a un grupo local derechos y permisos sobre los recursos situados en el mismo dominio donde ese grupo local haya sido definido. El empleo de ese grupo sólo podrá realizarse localmente en los servidores de su dominio. Un grupo local puede contener usuarios y grupos globales, pero no puede contener otros grupos locales.



También existen grupos locales en las estaciones de trabajo con Windows NT. Un grupo local de una estación de trabajo puede contener cuentas de usuario de la propia estación de trabajo, así como usuarios y grupos globales del dominio al que pertenece, y de otros dominios de su confianza.

Diferencias entre los grupos globales y locales

Aunque los grupos globales y locales desempeñan funciones similares, para su creación y utilización se aplican reglas diferentes.

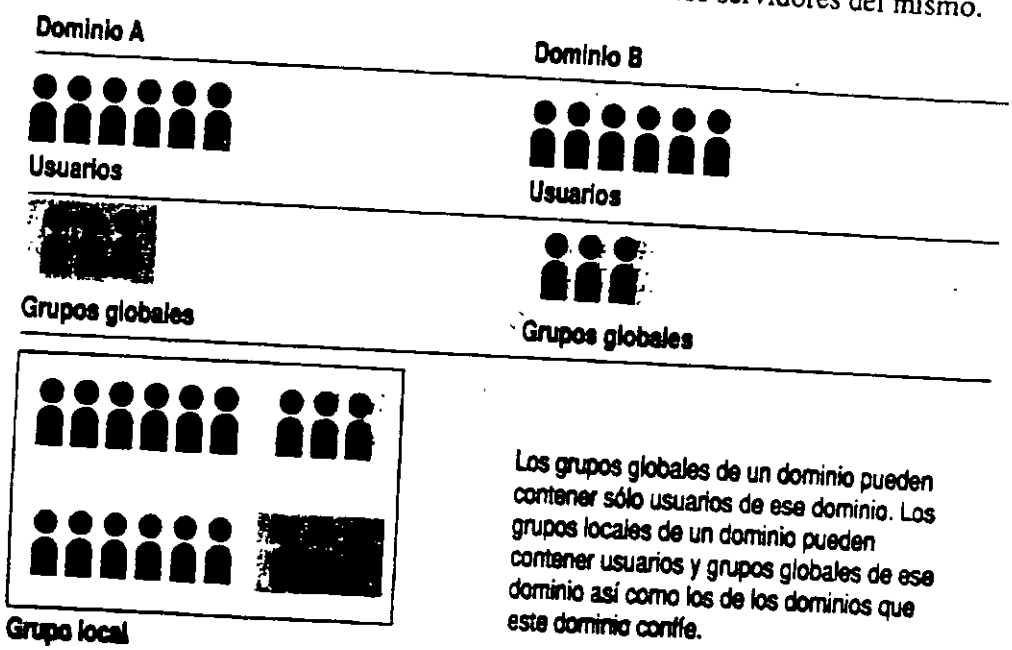
Un grupo global creado en el dominio Ventas:

- Sólo puede contener usuarios del dominio Ventas.
- Puede utilizarse en cualquier dominio que confíe en el dominio Ventas.

Un grupo local creado en el dominio Ventas.

- Puede contener usuarios y grupos globales del dominio Ventas y de cualquier dominio de confianza del dominio Ventas.
- Sólo puede utilizarse en servidores del dominio Ventas.

Obsérvese que los grupos locales de un dominio no pueden ser utilizados ni siquiera en las estaciones de trabajo con Windows NT pertenecientes a ese mismo dominio, ya que los grupos locales de un dominio son locales a los servidores del mismo.



Los términos "grupo global" y "grupo local" no se refieren al contenido del grupo, sino a los lugares donde el grupo puede recibir derechos y permisos (es decir, su *ámbito*).

Los grupos locales pueden contener grupos globales, pero los grupos globales pueden contener grupos locales u otros grupos globales.

Asimismo, la base de datos de cuentas de una estación de trabajo con Windows NT sólo puede contener grupos locales. En las estaciones de trabajo con Windows NT no existen grupos globales. Los grupos locales de una estación de trabajo con Windows NT sólo podrán recibir derechos y permisos en esa estación de trabajo. Aun cuando la estación de trabajo forme parte de un dominio, sus grupos locales no podrán utilizarse en ninguna otra computadora (ordenador).

strategias para el empleo de grupos locales y globales

Para facilitar la administración y el mantenimiento de su red, conviene que tenga en cuenta varias estrategias de utilización de grupos globales y grupos locales.

Si sus dominios están divididos de tal modo que cada uno de ellos corresponde a una división o departamento de la empresa, puede considerar como grupo local a un grupo de usuarios pertenecientes a un mismo departamento. (Recuerde que, en el Administrador de archivos y en el Administrador de usuarios para dominios, cuando se examinan grupos globales de un dominio que no es el dominio de observación actual, el nombre del grupo global aparece precedido por el nombre del dominio donde residen dicho grupo y sus miembros, por ejemplo Ventas\Directores.)

Este grupo de dominios puede recibir permisos y derechos en otros dominios, por lo que el concepto de grupo global constituye un medio para exportar este grupo de usuarios, como una misma unidad, a otros dominios (y estaciones de trabajo con Windows NT de la empresa). Cuando un administrador observe que el nombre del grupo aparece precedido por el nombre del dominio, sabrá tanto el tipo de personas que representa dicho grupo (observando el nombre del grupo) como el origen o ubicación del mismo (observando el nombre del dominio).

Un grupo local es un grupo que puede incluir usuarios y grupos globales procedentes de otros dominios, por lo que se trata de un modo de importar de una sola vez un conjunto de usuarios y grupos globales de otros dominios, para su utilización en el dominio local.

Como ejemplo de su aplicación, supongamos que el dominio Ingeniería posee un servidor en el cual existe un directorio compartido que contiene documentos que explican las nuevas tecnologías que está investigando la empresa. Los directores de otros departamentos (dominios) de la empresa están interesados en consultar estos documentos. Los administradores de la red podrán permitir esta posibilidad del siguiente modo:

1. Creando grupos globales en otros dominios (por ejemplo, Comercial\Directores y Ventas\Directores)
2. Creando un grupo local llamado "Todos los directores" en el dominio Ingeniería

3. Incorporando los grupos globales Comercial\Directores y Ventas\Directores al grupo local "Todos los directores"
4. Concediendo al grupo "Todos los directores" el permiso de lectura de los archivos de ese directorio

En el ejemplo anterior, lo cierto es que podríamos haber otorgado simplemente a cada uno de los grupos globales "Directores" de los otros dominios el permiso para leer los archivos, evitando la etapa de crear el grupo local. Sin embargo, en muchos casos la creación del grupo local ahorrará tiempo más adelante. Por ejemplo, supongamos que posteriormente se desea agregar dos nuevos directorios que contienen archivos de interés para los directores. Si no se hubiera creado el grupo local "Todos los directores", habría que conceder el acceso a los nuevos directorios a todos los grupos globales Directores, en lugar de hacerlo para un solo grupo local. El ahorro será mayor si el grupo local "Todos los directores" contiene muchos grupos globales, en lugar de sólo dos, como en este ejemplo.

Como puede observarse, un grupo local es una forma de reunir grupos globales y asignarles permisos a todos de una sola vez. De este modo, si algún otro grupo global necesita más adelante los mismos permisos que algún grupo global existente, bastará con agregar el nuevo grupo global al correspondiente grupo local, con lo cual dispondrá de todos los permisos que necesite.

Crear grupo para	Utilice	Comentarios
Agrupar usuarios de este dominio en una misma unidad, para utilizarla en otros dominios	Grupo global	El grupo global podrá incluirse en grupos locales o recibir permisos y derechos directamente en otros dominios.
Recibir permisos y derechos en un solo dominio	Grupo local	El grupo local puede contener usuarios y grupos globales de otros dominios.
Recibir permisos en estaciones de trabajo con Windows NT	Grupo global	Los grupos globales de un dominio podrán rescindir permisos en estaciones de trabajo con Windows NT, pero no los grupos locales de un dominio.
Contener otros grupos	Grupo local	El grupo local sólo puede contener grupos (y usuarios) globales; sin embargo, ningún grupo puede contener otros grupos locales.
Incluir usuarios de varios dominios	Grupo local	El grupo local sólo podrá utilizarse en el dominio en el cual haya sido creado. Si necesita otorgar a este grupo local permisos en varios dominios, deberá crear manualmente el grupo local en cada uno de los dominios donde lo necesite.

Estrategias para el empleo de grupos locales y globales incorporados

Las estrategias indicadas para el empleo de grupos locales y globales en general, descritas en la sección anterior, son aplicables también a los grupos globales y locales incorporados. Un ejemplo de ellos son los grupos globales "Administradores de dominios" y el grupo local "Administradores".

La pertenencia al grupo local "Administradores" es lo que convierte realmente a una cuenta en administrador de un dominio o estación de trabajo con Windows NT. Sin embargo, cuando se crea una cuenta en un dominio con Windows NT Advanced Server, existen dos formas de convertir esa cuenta en administrador: incluirla directamente en el grupo local "Administradores" o incluirla en el grupo global "Administradores de dominios", que a su vez es miembro de "Administradores".

Se recomienda encarecidamente utilizar siempre el segundo método: incluir la cuenta en el grupo global "Administradores de dominios". De este modo, se dispondrá de un grupo local que representará a todos los administradores del dominio. Ese grupo local podrá incluirse posteriormente en el grupo local "Administradores" de cualquier otro dominio, o de cualquier estación de trabajo con Windows NT, que los administradores de este dominio necesiten administrar. (En efecto, cuando se configura una estación de trabajo con Windows NT para integrarla en un dominio, el grupo global "Administradores de dominios" de ese dominio se incorpora automáticamente al grupo local "Administradores" de la estación de trabajo. Ello permite a los administradores del dominio realizar la administración de todas las estaciones de trabajo del mismo.)

Todo dominio incluye también un grupo global "Usuarios del dominio", en el cual se incluirán automáticamente todas las cuentas de usuario que se creen en el dominio, sin que sea necesario hacerlo explícitamente. Los grupos globales "Usuarios del dominio" son miembros automáticamente del grupo local "Usuarios" de su mismo dominio, como también son miembros del grupo local "Usuarios" de todas las estaciones de trabajo con Windows NT pertenecientes al dominio.

"Administradores de dominios" y "Usuarios del dominio" son los únicos grupos globales incorporados que se corresponden con grupos locales incorporados. Sin embargo, es posible crear otros grupos globales que se correspondan con grupos locales, si se desea utilizar las mismas estrategias para aquellos tipos de usuarios. Por ejemplo, puede ser interesante crear un grupo global "Operadores de copia de seguridad del dominio" para los operadores responsables de realizar las copias de seguridad en ese dominio. Posteriormente, si los operadores de copia de seguridad de ese dominio necesitan realizar copias de seguridad de los archivos de una estación de trabajo con Windows NT o de otro dominio, bastará con incorporar el grupo global "Operadores de copia de seguridad" al grupo local "Operadores de copia de seguridad" del dominio o de la estación de trabajo.

Distintos tipos de usuarios

Toda cuenta de usuario será (con toda probabilidad) miembro de uno o más grupos locales incorporados. La pertenencia a uno de los grupos locales incorporados de un dominio otorga a un usuario los derechos y facultades necesarios para realizar diversas tareas en los servidores del dominio. Análogamente, la pertenencia a un grupo incorporado de una estación de trabajo otorga al usuario derechos y facultades sobre esa estación de trabajo.

Para cada uno de los grupos locales incorporados, ciertas facultades son inherentes al grupo local y no pueden ser modificadas por ningún administrador, mientras que otras (las que se conceden al grupo local por medio de *derechos de usuario*) pueden ser modificadas por el administrador. En las tablas que se ofrecen en esta sección se muestra una perspectiva de las facultades de todos los grupos locales incorporados, tanto en dominios con Windows NT Advanced Server como en estaciones de trabajo con Windows NT. En las secciones siguientes se ofrecen más detalles sobre cada uno de los grupos locales.

Un usuario puede integrarse en más de un grupo incorporado. Con ello, el usuario adquirirá todas facultades que se hayan otorgado a esos grupos. Por ejemplo, un usuario que pertenezca tanto al grupo Operadores de impresión como a Operadores de copia de seguridad asumirá todos los derechos que hayan sido concedidos a los operadores de impresión, así como los derechos otorgados a los operadores de copia de seguridad.

Obsérvese que no todos los grupos locales incorporados aparecen tanto en las estaciones de trabajo con Windows NT como en los dominios con Windows NT Advanced Server. En la tabla siguiente se muestra qué grupos locales incorporados existen en los dominios y cuáles en las estaciones de trabajo con Windows NT.

Dominios con Windows NT Advanced Server	**Estaciones de trabajo con Windows NT**
Administradores	Administradores
Operadores de copia de seguridad	Operadores de copia de seguridad
Operadores de servidores	Usuarios avanzados
Operadores de cuentas	Usuarios
Operadores de impresión	Invitados
Usuarios	Duplicador
Invitados	
Duplicador	

En las tablas siguientes se indican los derechos y las facultades incorporadas correspondientes a cada uno de los grupos locales incorporados, tanto en dominios con Windows NT Advanced Server como en estaciones de trabajo Windows NT. Posteriormente se ofrece una descripción más detallada sobre el propósito y facultades de cada uno de los grupos locales incorporados.

Windows NT Advanced Server

● El grupo local tiene el derecho o facultad

○ El grupo local no tiene el derecho o facultad

	Administradores	Operadores de servidores	Operadores de cuentas	Operadores de impresión	Operadores de copia	Todos	Usuarios	Invitados
Derechos:								
Iniciar sesión local	●	●	●	●	●	○	○	○
Acceder a esta computadora desde la red	●	○	○	○	○	●	○	○
Tomar posesión de archivos	●	○	○	○	○	○	○	○
Administrar los registros de auditoría y seguridad	●	○	○	○	○	○	○	○
Cambiar la hora del sistema	●	●	○	○	○	○	○	○
Apagar el sistema	●	●	●	●	●	○	○	○
Forzar el apagado desde un sistema remoto	●	●	○	○	○	○	○	○
Hacer copias de seguridad de archivos y directorios	●	●	○	○	●	○	○	○
Restaurar archivos y directorios	●	●	○	○	●	○	○	○
Facultades incorporadas:								
Crear y administrar cuentas de usuario	●	○	●[1]	○	○	○	○	○
Crear y administrar grupos globales	●	○	●[1]	○	○	○	○	○
Crear y administrar grupos locales	●	○	●[1]	○	○	○	○	○
Asignar derechos a los usuarios	●	○	○	○	○	○	●[2]	○
Bloquear el servidor	●	●	○	○	○	●[3]	○	○
Desbloquear el servidor	●	●	○	○	○	○	○	○
Formatear el disco duro de la estación de trabajo	●	●	○	○	○	○	○	○
Crear grupos comunes	●	●	○	○	○	○	○	○
Mantener el perfil local	●	●	●	●	●	○	○	○
Compartir y dejar de compartir directorios	●	●	○	○	○	○	○	○
Compartir y dejar de compartir impresoras	●	●	○	●	○	○	○	○

[1] Los Operadores de cuentas no pueden modificar las cuentas de Administradores ni el grupo global de Administradores de dominio ni los grupos locales Operadores de copia, Administradores, Servidores, Operadores de cuentas u Operadores de impresión.

[2] Aunque los Usuarios tiene el derecho de crear grupos locales en un servidor, no podrán hacerlo a menos que tengan permisos para iniciar una sesión en un servidor local o tengan acceso a la herramienta Administrador de usuarios para dominios.

[3] Aunque Todos tienen derecho de bloquear el servidor, sólo esos usuarios que puedan iniciar una sesión en un servidor local podrán bloquearlo.

Estaciones de trabajo con Windows NT

● El grupo local tiene el derecho o facultad
○ El grupo local no tiene el derecho o facultad

	Administradores	Usuarios avanzados	Usuarios	Invitados	Todos	Operadores de copia
Derechos:						
Iniciar sesión local	●	●	●	●	●	●
Acceder a esta computadora desde la red	●	●	○	○	●	○
Tomar posesión de archivos	●	○	○	○	○	○
Administrar los registros de auditoría y seguridad	●	○	○	○	○	○
Cambiar la hora del sistema	●	●	○	○	○	○
Apagar el sistema	●	●	●	○	●	●
Forzar el apagado desde un sistema remoto	●	●	○	○	○	○
Hacer copias de seguridad de archivos y directorios	●	○	○	○	○	●
Restaurar archivos y directorios	●	○	○	○	○	●
Facultades incorporadas:						
Crear y administrar cuentas de usuario	●	●[1]	○	○	○	○
Crear y administrar grupos locales	●	●[2]	●[3]	○	○	○
Asignar derechos a los usuarios	●	○	○	○	○	○
Bloquear la estación de trabajo	●	●	○	○	●	○
Desbloquear la estación de trabajo	●	○	○	○	○	○
Formatear el disco duro de la estación de trabajo	●	○	○	○	○	○
Crear grupos comunes	●	●	○	○	○	○
Mantener el perfil local	●	●	○	○	○	●
Compartir y dejar de compartir directorios	●	●	○	○	○	○
Compartir y dejar de compartir impresoras	●	●	○	○	○	○

1 Un Usuario avanzado puede crear cuentas de usuario, pero sólo puede modificar y eliminar aquellas cuentas que ha creado personalmente.

2 Un Usuario avanzado puede crear grupos locales, así como agregar y eliminar usuarios de los grupos locales que ha creado personalmente y de los grupos locales Usuarios avanzados, Usuarios e Invitados. Sin embargo, no puede modificar los grupos locales Operadores de copia ni Administradores.

3 Los Usuarios pueden crear grupos locales, pero un Usuario puede modificar sólo los grupos locales que él o ella ha creado.

Administradores

Las cuentas del grupo local Administradores disponen de la autoridad necesaria para hacer prácticamente todo lo que deseen en los servidores que ejecuten Windows NT Advanced Server o en estaciones de trabajo con Windows NT. Entre estas posibilidades se incluye la creación, eliminación y administración de cuentas de usuario, grupos globales y grupos locales; la posibilidad de compartir directorios e impresoras; la concesión de permisos y derechos de uso de recursos a los usuarios; y la instalación de programas y archivos de sistemas operativos.

Obsérvese que, a diferencia de LAN Manager 2.x, los administradores no disponen de acceso automáticamente a cualquier archivo de un servidor: un administrador no podrá acceder a un archivo si los permisos del mismo no se lo autorizan. Todo archivo de un volumen NTFS posee un *propietario* que puede establecer los permisos sobre el archivo. Cuando se crea un archivo, su creador se convierte en propietario. No obstante, si es necesario un administrador podrá tomar posesión de un archivo y de este modo disponer de acceso al mismo. Si desea obtener más información sobre la propiedad de archivos y directorios, consulte el capítulo 5, "Administración de archivos de la red".

Como opción predeterminada, cuando una estación de trabajo con Windows NT se afilie a un dominio, el grupo global "Administradores de dominios" correspondiente a ese dominio será incorporado al grupo local "Administradores" de la estación de trabajo, lo cual permitirá a los administradores del dominio controlar todas las estaciones de trabajo con Windows NT de su dominio. Si desea impedir que los administradores de un dominio puedan administrar la estación de trabajo con Windows NT de un usuario, bastará con que elimine el grupo global "Administradores de dominios" del grupo local "Administradores" de la estación de trabajo.

Usuarios

Las cuentas del grupo local Usuarios son las de los usuarios habituales de la red, es decir, los que la utilizan para su trabajo. La mayoría de las cuentas de usuario que cree serán de este tipo.

Cuando en un dominio existan servidores que ejecuten Windows NT Advanced Server, los usuarios solamente podrán acceder a ellos a través de la red. No tendrán derecho a trabajar en los propios servidores.

Un miembro del grupo local Usuarios de una estación de trabajo con Windows NT podrá:

- Iniciar una sesión en esa estación de trabajo y utilizarla para acceder a la red.
- Bloquear y apagar la estación de trabajo.
- Mantener un perfil en la misma (si desea obtener más información sobre los perfiles, consulte el capítulo 4, "Administración de entornos de usuario").
- Crear y eliminar grupos locales en la estación de trabajo.
- Modificar la pertenencia a los grupos locales que haya creado (pero no podrá modificar los grupos locales incorporados ni los grupos locales creados por alguna otra persona).

Invitados

En un servidor con Windows NT Advanced Server, los miembros del grupo Invitados poseen los mismos derechos que los del grupo Usuarios: ambos grupos sólo pueden acceder al servidor a través de la red y no pueden iniciar una sesión localmente en el servidor.

Los invitados tienen menos derechos que los usuarios cuando trabajan en estaciones de trabajo con Windows NT. Los usuarios pueden mantener un perfil local en su estación de trabajo, bloquear la estación de trabajo y crear, eliminar y modificar grupos locales en la estación de trabajo, mientras que los invitados no pueden hacer ninguna de estas cosas.

Operadores de servidores

El grupo local Operadores de servidores solamente existirá en aquellos servidores que estén ejecutando Windows NT Advanced Server, no en las estaciones de trabajo con Windows NT. La principal misión de los operadores de servidores es mantener en funcionamiento los servidores de la red.

Las facultades de las cuentas del grupo local Operadores de servidores son muy similares a las de los administradores, excepto que no pueden administrar la seguridad en el servidor. En especial, los operadores de servidores pueden compartir y dejar de compartir archivos e impresoras de un servidor, bloquear o saltar el bloqueo de un servidor, así como dar formato a los discos del servidor. También pueden iniciar una sesión en los servidores, realizar copias de seguridad y restaurar los archivos de un servidor, o apagar servidores.

Operadores de cuentas

El grupo local Operadores de cuentas sólo existirá en los servidores que ejecuten Windows NT Advanced Server, no en las estaciones de trabajo con Windows NT.

Las cuentas del grupo local "Operadores de cuentas" de un servidor pueden administrar las cuentas de grupo y de usuario del servidor. Un operador de cuentas puede crear, eliminar y modificar prácticamente a todos los usuarios, grupos globales y grupos locales. No obstante, existen algunas excepciones: los operadores de cuentas no pueden modificar las cuentas de usuario del grupo Administradores, como tampoco las de los grupos locales Administradores, Operadores de servidores, Operadores de cuentas, Operadores de impresión ni Operadores de copia de seguridad. Tampoco pueden asignar derechos a los usuarios.

Operadores de impresión

El grupo local Operadores de impresión sólo existirá en los servidores que ejecuten Windows NT Advanced Server, no en las estaciones de trabajo con Windows NT.

Las cuentas del grupo local Operadores de impresión pueden compartir y dejar de compartir impresoras, así como administrar las impresoras compartidas de los servidores que ejecuten Windows NT Advanced Server. También pueden iniciar sesiones localmente en los servidores, así como apagarlos.

Si desea que los operadores de impresión de un dominio se encarguen de administrar las impresoras controladas por las estaciones de trabajo con Windows NT del dominio, así como las impresoras controladas por los servidores del dominio, realice las siguientes operaciones:

1. Cree un grupo global llamado "Operadores de impresión del dominio" en el dominio. Convierta este grupo global en miembro del grupo local "Operadores de impresión".
2. Agregue las cuentas de usuario de cada uno de los operadores de impresión al grupo global "Operadores de impresión del dominio".
3. En cada estación de trabajo que controle impresoras, agregue el grupo global "Operadores de impresión del dominio" al grupo local "Usuarios avanzados" en la estación de trabajo.

Operadores de copia de seguridad

Las cuentas del grupo "Operadores de copia de seguridad" de un servidor o estación de trabajo pueden realizar copias de seguridad de los archivos de la computadora (ordenador), así como también restaurar dichos archivos.

Tanto en los servidores que ejecuten Windows NT Advanced Server como en las estaciones de trabajo con Windows NT, los Operadores de copia de seguridad pueden realizar copias de seguridad de archivos, restaurar archivos, iniciar sesiones localmente en la computadora y apagar la computadora.

Usuarios avanzados

El grupo local Usuarios avanzados sólo existirá en las estaciones de trabajo con Windows NT, no en los servidores que ejecuten Windows NT Advanced Server.

Un miembro del grupo local Usuarios avanzados puede hacer todo lo que está permitido para un miembro del grupo Usuarios y, además, puede crear cuentas de usuario; modificar cuentas de usuario que haya creado; incluir cuentas de usuario de la estación de trabajo en los grupos incorporados Usuarios avanzados, Usuarios e Invitados; así como compartir y dejar de compartir archivos e impresoras situados en la estación de trabajo.

Puesto que el grupo Usuarios avanzados sólo existe en las estaciones de trabajo con Windows NT, pero no en los servidores, una estrategia habitual de utilización de este grupo consiste en incluir la cuenta de dominio de cada usuario en el grupo "Usuarios avanzados" de su respectiva estación de trabajo. Por ejemplo, supongamos que la cuenta de dominio LuisaE se incorpora al grupo "Usuarios avanzados" de su estación de trabajo. En los servidores del dominio, LuisaE se convertirá automáticamente en miembro del grupo Usuarios. De este modo, LuisaE dispondrá de un mayor grado de control sobre su propia estación de trabajo y, además podrá compartir sus archivos con otros usuarios, aunque en los servidores de su dominio LuisaE será un usuario normal.

En general, la cuenta de cualquier usuario normal pasará a formar parte del grupo "Usuarios" del propio dominio. En la estación de trabajo de cada usuario es posible decidir si la cuenta de dominio del usuario se incorporará al grupo Usuarios avanzados (para permitirle controlar la estación de trabajo en mayor medida) o al grupo Usuarios (para que pueda disponer de un menor grado de control).

Puesto que el grupo Usuarios avanzados sólo existe en estaciones de trabajo con Windows NT y no en dominios con Windows NT Advanced Server, el concepto de usuario avanzado no tiene ningún sentido para aquellos usuarios que utilicen estaciones de trabajo con MS-DOS.

Duplicador

El último grupo integrado, Duplicador, sólo se utiliza en combinación con el servicio Duplicador de archivos. Si no va a utilizar el Duplicador de archivos, no necesitará administrar el grupo local Duplicador. Para obtener más información sobre la duplicación de archivos, consulte el capítulo 5, "Administración de archivos de la red".

Cuentas incorporadas

Cuando se instala Windows NT Advanced Server en un servidor o Windows NT en una estación de trabajo, se incorporan a la base de datos de cuentas de la computadora (ordenador) varias cuentas predeterminadas de usuario, grupos globales y grupos locales. En las secciones siguientes se describen cada una de estas cuentas predeterminadas y la utilidad de las mismas.

Cuentas de usuario incorporadas

Inicialmente, en cualquier computadora con Windows NT o Windows NT Advanced Server existen dos cuentas de usuario predeterminadas: Administrador e Invitado.

Administrador es la cuenta que podrá utilizar la primera vez que realice tareas de administración en un nuevo servidor de estación de trabajo, antes de crear su propia cuenta personal. La cuenta Administrador no se puede eliminar ni desactivar, lo cual le garantiza que nunca se quedará bloqueado sin poder usar su computadora por haber eliminado o desactivado todas las cuentas administrativas.

Invitado es una cuenta que se utiliza para *inicios de sesión de invitados*, es decir, realizados por personas que no dispongan de una cuenta en la computadora, en el dominio al que pertenecen, ni en ninguno de sus dominios de confianza. La cuenta Invitado queda desactivada automáticamente cuando se instala Windows NT o Windows NT Advanced Server, pero puede activarse si se desea permitir que los invitados puedan iniciar sesiones. Para obtener más información al respecto, consulte la sección "Autorización de acceso a invitados", más adelante en este mismo capítulo.

Cuenta	¿Puede eliminarse?	¿Puede desactivarse?	¿Puede cambiarse de nombre?
Administrador	No	No	Sí
Invitado	No	Sí	Sí

Grupos globales incorporados

En Windows NT Advanced Server existen dos grupos globales incorporados: "Administradores de dominios" y "Usuarios del dominio". Ninguno de estos grupos puede eliminarse.

"Administradores de dominios" contiene inicialmente la cuenta Administrador. Cuando cree cuentas para los administradores de su dominio, deberá agregarlas al grupo global "Administradores de dominios", en lugar de incluirlas simplemente en el grupo local Administradores. Para obtener más información al respecto, consulte "Estrategias para el empleo de grupos locales y globales incorporados", sección anterior de este mismo capítulo.

Inicialmente, "Usuarios del dominio" incluirá las cuentas predeterminadas Administrador e Invitado. Cualquier cuenta de usuario que se incorpore a este dominio más adelante será incluida automáticamente en el grupo global "Usuarios del dominio".

Grupo global	Contenido inicial	¿Quién puede modificarla?[1]
Administradores de dominios	Administrador	Administradores
Usuarios del dominio	Administrador	Administradores, operadores de cuentas

[1] Ninguno de los grupos puede ser eliminado.

Grupos locales incorporados

Cuando se instala Windows NT Advanced Server en un servidor o Windows NT en una estación de trabajo, se crean varios grupos locales predeterminados. La pertenencia a uno de estos grupos locales otorga a un usuario determinadas facultades. Las facultades de cada grupo local se describen en "Distintos tipos de usuarios", sección anterior de este mismo capítulo. Ninguno de estos grupos locales incorporados puede eliminarse.

Además de estos grupos locales, existe una identidad llamada "Todos" que representa a todos los miembros de la red, incluyendo los administradores, todo tipo de operadores, usuarios, usuarios de otros dominios e invitados. La pertenencia al grupo "Todos" no puede modificarse. Este grupo contiene siempre a todos los usuarios automáticamente. "Todos" no es en realidad un grupo local y no aparece como tal en la lista de grupos del Administrador de usuarios, pero es posible asignarle permisos de archivos (en el Administrador de archivos) o derechos (en el cuadro de diálogo **Derechos** del Administrador de usuarios para dominios).

En la tabla siguiente se muestra los grupos locales incorporados existentes tanto en los servidores ejecutando Windows NT Advanced Server como en las estaciones de trabajo ejecutando Windows NT.

Grupos locales incorporados en servidores

Grupo	Contenido inicial	¿Quién puede modificarla?[1]
Servidores:		
Administradores	Administradores de dominios (grupo global) Administrador (cuenta de usuario)	Administradores
Usuarios	Usuarios del dominio (grupo global) Administrador (cuenta de usuario)	Administradores, Operadores de cuentas
Invitados	Invitado (cuenta de usuario)	Administradores, Operadores de cuentas
Operadores de servidores	Ninguno	Administradores
Operadores de impresión	Ninguno	Administradores
Operadores de copia de seguridad	Ninguno	Administradores
Operadores de cuentas	Ninguno	Administradores
Duplicador	Ninguno	Administradores, Operadores de cuentas, Operadores de servidores
Estaciones de trabajo:		
Administradores	Administrador (cuenta de usuario)[2]	Administradores
Usuarios	Ninguno	Administradores, Usuarios avanzados

Estaciones de trabajo:

Grupo	Contenido inicial	¿Quién puede modificarla?[1]
Usuarios avanzados	Usuario de instalación[3]	Administradores, Usuarios avanzados
Invitados	Invitados (cuenta de usuario)	Administradores, Usuarios avanzados
Operadores de copia de seguridad	Ninguno	Administradores
Duplicador	Ninguno	Administradores

[1] Ninguno de los grupos puede ser eliminado.

[2] Si se ha configurado la estación de trabajo para que forme parte de un dominio, los grupos globales "Administradores de dominios" correspondientes a ese dominio serán incorporados automáticamente al grupo local "Administradores" de la estación de trabajo.

[3] "Usuario de instalación" es una cuenta cuyo nombre de usuario es especificado durante la instalación de Windows NT por la persona que realice esta operación. Esta cuenta sólo existirá si la estación de trabajo no se incluyó en un dominio en el momento en que se instaló Windows NT en ella.

Control de las facultades de los usuarios

Existen varias formas de controlar lo que los usuarios pueden y no pueden hacer, en sus estaciones de trabajo y en el resto de la red. El método más importante y el que utilizará con mayor frecuencia consiste en emplear grupos locales predefinidos. Con sólo incorporar un usuario a alguno de estos grupos, podrá otorgársele un gran conjunto de facultades y derechos predefinidos. Para obtener más información sobre lo que cada uno de los grupos locales predefinidos permite hacer, consulte "Distintos tipos de usuarios", sección anterior de este mismo capítulo.

Otra forma de limitar las facultades de los usuarios es configurar determinadas opciones en sus respectivas cuentas, como la limitación de las horas de conexión y las estaciones de trabajo que estarán autorizados a emplear.

Los *permisos* de cada archivo, directorio o impresora compartido de la red definen quién puede acceder a tales recursos y quién no. Es posible asignar permisos a grupos locales, grupos globales y directamente a usuarios individuales, pero se recomienda no asignar permisos a usuarios individuales, excepto en raras ocasiones, ya que resultan más difíciles de mantener.

Las actividades de los usuarios pueden controlarse mediante la *auditoría* de acciones y recursos. La auditoría de una acción o recurso provoca la anotación de una entrada en el registro de sucesos de seguridad cada vez que se realice la acción correspondiente o se acceda al recurso indicado, lo cual garantiza que los usuarios serán los responsables de sus propias acciones.

Es posible manipular directamente los *derechos de usuario* (también llamados simplemente *derechos*), que especifican las acciones que pueden realizar los grupos locales, grupos globales y usuarios. Sin embargo, se recomienda no hacerlo más que en contadas ocasiones. En lugar de ello, es mejor utilizar los grupos locales predefinidos, con sus conjuntos predeterminados de derechos. Estos grupos serán suficientes para atender la mayoría de las necesidades. Sin embargo, si realmente desea conceder derechos a otros grupos o usuarios, o regular de un modo muy específico los derechos de los grupos predeterminados, puede hacerlo.

Por último, existe otro método que permite modificar sustancialmente el entorno del escritorio de un usuario de Windows NT: la asignación de un *perfil* de usuario. Para obtener más información sobre los perfiles, consulte el capítulo 4, "Administración de entornos de usuario".

Permisos

El Administrador de archivos se puede utilizar para especificar los permisos de los archivos en particiones NTFS, tanto de servidores ejecutando Windows NT Advanced Server como de estaciones de trabajo con Windows NT. Estos permisos se aplicarán tanto a los usuarios que trabajen en la misma computadora (ordenador) como a aquellos que accedan a los archivos a través de la red (en caso de que sean compartidos). Es posible establecer permisos sobre archivos hasta un nivel de granularidad muy detallado. Por ejemplo, se pueden establecer distintos permisos para cada uno de los archivos de un directorio, si se desea. También es posible establecer muchos tipos de permisos diferentes. Por ejemplo, se puede permitir que un usuario lea el contenido de un archivo y lo modifique, mientras que otro sólo pueda leerlo, y al mismo tiempo impedir que los demás usuarios tengan acceso a ese archivo.

Este tipo de restricciones de acceso no estará disponible en particiones FAT o HPFS en computadoras con Windows NT. Los archivos de estas particiones pueden ser leídos y modificados por cualquier usuario que trabaje en la propia computadora. Sin embargo, sí es posible proteger los directorios compartidos de las particiones FAT o HPFS, especificando un conjunto de permisos que se apliquen a los usuarios de todos los archivos y subdirectorios del directorio compartido. Se trata de los *permisos de recurso compartido*.

Para obtener más información sobre los permisos de archivos y los permisos de recurso compartido, consulte el capítulo 5, "Administración de archivos de la red".

También pueden establecerse tipos de permisos similares para las impresoras compartidas que sean administradas por computadoras con Windows NT Advanced Server. Para obtener más información al respecto, consulte el capítulo 6, "Uso compartido de impresoras".

Permisos del Visor del portafolio

El Visor del portafiolio le permite compartir información entre diferentes aplicaciones y usuarios, y vincula e incrusta en forma dinámica esa información en otros archivos y documentos en la misma computadora, o en otras computadoras que tengan Windows NT. Para obtener más información acerca el Visor del portafolio, y de la vinculación e incrustación de objetos (OLE), consulte el *Manual de sistema de Microsoft Windows NT Advanced Server.*

Cuando se transfiere una parte de la información al Visor del portafolio, esta información toma el formato de una *página.* El Visor del portafolio puede contener hasta 127 páginas, las mismas que se pueden compartir con otros usuarios. El usuario que crea una página puede establecer permisos para dicha página, los cuales especifican si otros usuarios pueden hacer uso de ella.

Para crear, compartir o dejar de compartir, y eliminar una página del Visor de portafolio, el usuario debe estar en uno de los siguientes grupos en la computadora:

- Administradores
- Operadores de servidor
- Usuarios avanzados
- Usuarios

Además, el grupo especial Todos puede utilizar el Visor del portafolio para ver la lista de páginas compartidas en la computadora.

Cuando el usuario crea y comparte una página nueva en el Visor del portafolio, ese usuario se convierte en el propietario de la misma y los siguientes permisos son configurados en forma predeterminada en la página. El propietario de la página puede cambiar dichos permisos si el o ella así lo desea.

Permisos para la página nueva del Visor del portafolio

Usuario o grupo	Permisos
Nombre de usuario del creador/propietario	Control total
Todos	Lectura y vinculación

La siguiente lista muestra los tipos de permisos que se pueden establecer en las páginas del Visor del portafolio. Se puede conceder permisos diferentes a los distintos usuarios, de esta forma otorgando acceso a algunas personas y negándoles a otras.

- Sin acceso
- Lectura
- Lectura y vinculación
- Modificación
- Control total

Auditoría

Es posible especificar que cada vez que se realicen determinadas acciones o se acceda a ciertos archivos, se efectúe una anotación de auditoría en el registro de sucesos de seguridad. En la anotación de auditoría se mostrará la acción realizada, el usuario responsable, y la fecha y hora en que tuvo lugar. Es posible someter a auditoría tanto los intentos que han logrado su propósito como los intentos fallidos, por lo que el registro cronológico de auditoría puede indicar tanto las personas que llevaron a cabo realmente determinadas acciones en la red como los que intentaron ejecutarlas y no fueron autorizados.

La siguiente tabla muestra las ventajas y desventajas de la utilización del modelo de dominio maestro.

Ventajas	Desventajas
Es la opción más indicada para empresas que tengan menos de 10.000 usuarios y necesiten que los recursos compartidos se dividan en grupos.	No puede utilizarse en empresas con más de 10.000 usuarios.
Permite administrar las cuentas de usuario de manera centralizada.	Obliga a definir grupos locales en cada uno de los dominios donde vayan a utilizarse.
Los recursos se agrupan de una manera lógica.	
Los dominios de los distintos departamentos pueden tener sus propios administradores, que se encargarán de controlar los recursos del departamento.	
Sólo es necesario definir los grupos globales una vez (en el dominio maestro).	

Existe una variante de este modelo que puede utilizarse en empresas en las cuales existan varias divisiones diferentes, cada una de ellas con su propia administración de sistema de información (MIS). En este caso, las distintas divisiones tendrían sus respectivos dominios maestros, cada uno de los cuales englobaría a los usuarios que trabajen en la división respectiva. Cada uno de los dominios departamentales confiará probablemente en un solo dominio maestro: el dominio maestro de la división a la cual pertenezca dicho departamento. Sin embargo, si un dominio departamental lo necesita, podrá confiar en más de un dominio maestro. Los dominios maestros probablemente no necesitarán confiar entre sí.

Modelo de dominio maestro múltiple

En empresas de gran tamaño que deseen disponer de administración centralizada, el modelo de dominio maestro múltiple puede ser la opción más indicada, ya que es el que ofrece mayores posibilidades de ampliación.

En este modelo existe un número reducido de dominios maestros. Los dominios maestros actúan como dominios de cuentas. Toda cuenta de usuario de la red será creada en alguno de estos dominios maestros. La administración de sistema de información (MIS) de la empresa podrá administrar los dominios maestros. Aparte de los dominios maestros, existirán otros, los dominios departamentales, que proporcionarán recursos. Los dominios departamentales podrán ser administrados por los miembros del departamento respectivo o bien, por el departamento de MIS.

En la tabla siguiente se muestran las categorías de sucesos que pueden configurarse para ser auditados, así como los sucesos incluidos dentro de cada una de estas categorías. Para cada categoría puede optarse por auditar únicamente las acciones correspondientes a esa categoría que se hayan realizado con éxito, las que no han llegado a ejecutarse, ambas o ninguna de ellas.

Categoría	Sucesos
Inicio y cierre de sesión	Intentos de iniciar una sesión, intentos de cerrar una sesión, creación e interrupción de conexiones de red con los servidores
Acceso a archivos y objetos	Accesos realizados sobre un directorio o archivo configurado para su auditoría en el Administrador de impresión; utilizaciones de una impresora administrada por la computadora (ordenador)
Empleo de derechos de usuario	Aplicación de derechos de usuario con éxito; intentos fallidos de utilizar derechos no asignados a un usuario
Administración de usuarios y grupos	Creación, eliminación y modificación de cuentas de usuario y de grupo
Cambios en el plan de seguridad	Concesión o revocación de derechos de usuario para grupos y usuarios; establecimiento y ruptura de relaciones de confianza con otros dominios
Reinicio, apagado y sistema	Veces que se ha apagado o reiniciado la computadora; saturación del registro de auditoría; veces en que se han descartado anotaciones de auditoría cuando el registro de auditoría está saturado
Seguimiento de procesos	Inicios y detenciones de procesos en la computadora

Para especificar los tipos de sucesos de sistema que se someterán a auditoría, utilice el Administrador de usuarios. Para especificar los archivos que se auditarán y la forma en que serán auditados (siempre y cuando se haya utilizado el Administrador de usuarios para activar la auditoría de accesos a archivos), utilice el Administrador de archivos.

La siguiente tabla muestra los tipos de accesos a los directorios y archivos que se pueden auditar.

Acceso a directorios	Acceso a archivos
Mostrar los nombres de los archivos de un directorio	Mostrar los datos del archivo
Mostrar los atributos de un directorio	Mostrar los atributos del archivo
Cambiar los atributos de un directorio	Mostrar el propietario y los permisos del archivo
Crear subdirectorios y archivos	Modificar el archivo
Ir a los subdirectorios de un directorio	Modificar los atributos del archivo
Mostrar el propietario y los permisos de un directorio	Ejecutar el archivo
Eliminar el directorio	Eliminar el archivo
Cambiar los permisos de un directorio	Cambiar los permisos del archivo
Cambiar la posesión de un directorio	Cambiar la posesión del archivo

Derechos de usuario

Los derechos de usuario permiten determinar quién podrá realizar diversos tipos de acciones en las estaciones de trabajo con Windows NT y servidores ejecutando Windows NT Advanced Server. Entre las acciones gobernadas en virtud de los derechos se incluye, la facultad de iniciar una sesión localmente en la computadora (ordenador), apagarla, ajustar la hora de su reloj interno, realizar copias de seguridad de los archivos del servidor y restaurar dichos archivos, así como otras operaciones.

En servidores ejecutando Windows NT Advanced Server, la concesión y revocación de derechos se aplica a nivel de dominio. Así, si un grupo posee un derecho en un dominio, sus miembros adquirirán tal derecho en todos los servidores del dominio (pero no en las estaciones de trabajo con Windows NT pertenecientes a ese dominio). En una estación de trabajo con Windows NT, los derechos concedidos sólo se aplicarán a esa computadora individual.

Derechos	Comentarios	Se concede a: Servidores	Se concede a: Estaciones de trabajo
Administrar los registros de auditoría y seguridad	Permite especificar los tipos de sucesos y accesos a archivos que se someterán a auditoría. Permite ver y eliminar el registro de seguridad.	Administradores	Administradores
Hacer copias de seguridad de archivos y directorios		Administradores, Operadores de servidores, Operadores de copia de seguridad	Administradores, Operadores de copia de seguridad
Restaurar archivos y directorios	Obsérvese que este derecho prevalece sobre los permisos del archivo; un usuario que disponga del derecho Restauración podrá sobrescribir archivos para los cuales no posea los permisos necesarios, cuando realice una operación de restauración.	Administradores, Operadores de servidores, Operadores de copia de seguridad	Administradores, Operadores de copia de seguridad
Cambiar la hora del sistema		Administradores, Operadores de servidores	Administradores, Usuarios avanzados
Acceder a esta computadora desde la red	Permite acceder a la computadora desde otra estación de trabajo de la red.	Administradores, Todos	Administradores, Usuarios avanzados, Todos
Iniciar sesión localmente	Permite iniciar una sesión en la propia computadora, utilizando el teclado de la misma.	Administradores, Operadores de servidores, Operadores de cuentas, Operadores de impresión, Operadores de copia de seguridad	Administradores, Operadores de copia de seguridad, Usuarios avanzados, Usuarios, Invitados
Apagar el sistema		Administradores, Operadores de servidores, Operadores de cuentas, Operadores de impresión, Operadores de copia de seguridad	Administradores, Operadores de copia de seguridad, Usuarios avanzados, Usuarios, Invitados

Derechos	Comentarios	Se concede a: Servidores	Se concede a: Estaciones de trabajo
Tomar posesión de archivos y otros objetos	Permite tomar posesión de archivos y directorios de la computadora.	Administradores	Administradores
Forzar el apagado desde un sistema remoto	Este derecho no ofrece al usuario ninguna facultad en la versión actual de Windows NT, aunque será incorporado en futuras versiones del sistema operativo.	Administradores, Operadores de servidores	Administradores, Usuarios avanzados

Si desea consultar las tablas en las que aparecen los derechos asignados a los grupos locales incorporados, consulte "Distintos tipos de usuarios", sección anterior de este mismo capítulo.

Es posible conceder o revocar derechos a usuarios y grupos locales. Otras facultades no son directamente controlables por usted, ya que se conceden a ciertos grupos locales incorporados en el momento de la instalación de Windows NT o Windows NT Advanced Server. La única forma de conceder a un usuario una de estas facultades incorporadas es convertirle en miembro del grupo local correspondiente. Por ejemplo, el único modo de permitir a alguien que cree cuentas de usuario en un servidor es convertirle en miembro de los grupos locales "Administradores" u "Operadores de cuentas" de ese servidor.

Aunque se dispone de la facultad de conceder y revocar derechos a grupos locales, grupos globales y usuarios individuales (utilizando el Administrador de usuarios o el Administrador de usuarios de dominios), en la mayoría de los casos es mejor no hacerlo. Si desea conceder a un usuario la facultad de realizar determinadas acciones, es preferible que incluya a dicho usuario en el correspondiente grupo local predefinido (por ejemplo Administradores, Operadores de impresión, Usuarios avanzados y Usuarios). Estos grupos incorporan un conjunto de derechos cuidadosamente planificados que seguramente le resultarán de gran utilidad. Una situación en la que puede interesar modificar la forma en que se configuran los derechos se explica en la sección "Autorización de acceso a invitados", más adelante en este mismo capítulo.

Además de los derechos de usuario indicados en la tabla anterior, existen otros *derechos de usuario avanzados*, que probablemente no necesite utilizar con tanta frecuencia. Muchos de estos derechos avanzados solamente resultarán útiles para programadores que desarrollen aplicaciones para Windows NT y no deben concederse a ningún usuario ni grupo local. Estos derechos se muestran en la tabla siguiente. Si desea obtener más información sobre su utilización por parte de los programadores, consulte la documentación de programación de Windows NT.

- Actuar como parte del sistema operativo
- Crear un archivo de paginación
- Crear objetos testigo
- Crear objetos compartidos permanentes
- Depurar programas
- Generar auditorías de seguridad
- Incrementar cuotas
- Cargar y descargar controladores de dispositivo
- Bloquear páginas en memoria
- Modificar los valores de entorno de la memoria no volátil *(firmware)*
- Perfilar el sistema
- Reemplazar un testigo a nivel de proceso

Existen otros derechos avanzados que sí resultan interesantes para los administradores. Se explican en la tabla siguiente.

Derechos de usuario avanzados

Derecho	Definición	Concedido inicialmente a
Omitir la comprobación de movimiento transversal	Permite a un usuario cambiar de directorio a través de un árbol de directorios, incluso aunque no disponga de permisos para alguno de estos directorios.	Todos
Iniciar sesión como servicio	Permite a un proceso registrarse como servicio dentro del sistema. Este derecho es útil cuando se configura el servicio Duplicador. Si desea obtener más información al respecto, consulte el capítulo 5, "Administración de archivos de la red".	Ninguno

Configuración del plan de cuentas y contraseñas

Para cada dominio, es posible especificar todos los aspectos de la política de contraseñas: longitud mínima de la contraseña (el valor predeterminado es de 6 caracteres), duración mínima y máxima de la contraseña (los valores predeterminados son de 14 y 30 días, respectivamente), y repetibilidad de la contraseña, que impide a un usuario sustituir su contraseña por otra que haya utilizado recientemente (la opción predeterminada es impedir que los usuarios puedan utilizar de nuevo sus 3 últimas contraseñas).

Nota Si está utilizando la opción de repetibilidad de contraseñas como parte de su plan de contraseñas, asegúrese de configurar una duración mínima para las contraseñas lo bastante alta como para impedir que los usuarios puedan reciclar varias contraseñas temporales hasta obtener su contraseña favorita.

También puede especificar si desea que los usuarios sean obligados a desconectarse de los servidores del dominio cuando termine el horario durante el cual están autorizados a conectarse. Si lo hace, los usuarios recibirán advertencias justo antes de que termine el período de conexión que tengan especificado; por consiguiente, si por entonces aún no han cerrado sus conexiones, el servidor o servidores a los cuales estén conectados se encargarán de cerrarlas. Sin embargo, no se obligará a los usuarios a cerrar su sesión en su estación de trabajo.

Inicio de sesión de los administradores

Prácticamente todos los administradores de redes desempeñan un doble papel: actúan tanto de administradores como de usuarios de la red. Aunque en determinados casos realizarán tareas propias de la administración de la red, en otros serán simplemente usuarios de la red, ejecutando las mismas tareas que otros usuarios.

Por este motivo, es conveniente que cada administrador disponga en realidad de dos cuentas de usuario. Una de ellas estará incluida en el grupo Administradores y podrá ser la cuenta que utilice el administrador cuando necesite realizar tareas relacionadas con la administración de la red. La otra cuenta se encontrará en el grupo "Usuarios del dominio" y será la que utilizará el administrador en las demás ocasiones, cuando no esté realizando tareas de administración de la red.

Si sus administradores utilizan dos cuentas de este modo, la red será más segura. Mientras esté conectado como usuario normal, un administrador no podrá modificar accidentalmente ninguno de los aspectos de la red que sólo los administradores pueden cambiar. Además, si el administrador introduce un virus o un caballo de Troya, tal programa no poseerá los derechos de administrador y no conseguirá modificar el software del sistema operativo.

El empleo de este método reduce en cierto modo la facilidad de uso para los administradores, ya que les obliga a cerrar una sesión y volver a iniciarla para poder realizar tareas de administración de la red.

Autorización de acceso a invitados

Como opción predeterminada, todos los dominios con Windows NT Advanced Server y toda estación de trabajo con Windows NT tendrán definida (y desactivada) una cuenta Invitado. La cuenta Invitado no tiene ninguna contraseña y puede utilizarse para dos clases de inicios de sesión por parte de los invitados: *inicios de sesión de invitado locales* e *inicios de sesión de invitado de la red*. Cada estación de trabajo y cada dominio pueden configurarse para permitir ambos tipos de accesos por parte de los invitados, sólo uno o ninguno de ellos.

Funcionamiento de los inicios de sesión de invitados locales

Un *inicio de sesión de invitado local* tendrá lugar cuando un usuario que trabaje en una estación de trabajo con Windows NT o en un servidor con Windows NT Advanced Server especifique Invitado como nombre de usuario en el cuadro de diálogo de inicio de sesión, en el momento de dar comienzo a la misma. El usuario invitado podrá trabajar en esa computadora (sujeto a los derechos y permisos que se hayan concedido a la cuenta Invitado) y utilizarla para acceder a la red.

Funcionamiento de los inicios de sesión de invitados de la red

Un *inicio de sesión de invitado de la red* tendrá lugar en una computadora (ordenador) cuando un usuario procedente de un dominio en el que no confía esa computadora intente acceder a la misma a través de la red. La computadora que permite al invitado de la red iniciar una sesión no reconocerá la cuenta que está intentando acceder a ella, ya que dicha computadora no confía en ese dominio. Lo que hará es autorizar un inicio de sesión de invitado (siempre y cuando la cuenta Invitado de la computadora de destino no tenga ninguna contraseña). Con ello, el usuario invitado adquirirá todos los derechos, permisos y pertenencias a grupos de la computadora que hayan sido concedidos a la cuenta Invitado, incluso aunque dicho usuario invitado no haya especificado como nombre de usuario la palabra Invitado.

Obsérvese que, si una red de Windows NT Advanced Server se ha configurado de tal modo que todas las cuentas de usuario estén definidas en dominios de Windows NT Advanced Server en los que confían todos los demás dominios, en muy raras ocasiones se realizarán inicios de sesiones de invitado de red en ningún servidor, ya que este tipo de inicios de sesión sólo podrá producirse cuando un usuario de un dominio en el que no confía intente acceder a la computadora. (Sin embargo, sí podrán producirse inicios de sesión de invitado de la red con las cuentas de usuario que estén almacenadas en estaciones de trabajo con Windows NT, o cuando un usuario de una estación de trabajo con LAN Manager 2.x o Windows para Trabajo en grupo inicie una sesión de forma autónoma y posteriormente obtenga acceso a un servidor con Windows NT Advanced Server.)

Administración de inicios de sesión de invitados

Si no desea permitir inicios de sesión de invitados locales o de la red en un dominio de servidores con Windows NT Advanced Server o en una estación de trabajo con Windows NT, no es necesario que haga nada especial, ya que, como opción predeterminada, la cuenta Invitado está desactivada. Si desea permitir tanto los inicios de sesión locales como los remotos, bastará con que utilice el Administrador de usuarios para dominios para activar la cuenta Invitado. Para autorizar los inicios de sesión de invitados locales pero no los de invitados de la red, active la cuenta Invitado pero revoque su derecho "Acceder a esta computadora desde la red". Si lo que desea es permitir los inicios de sesión de invitados de la red pero no los locales, active la cuenta Invitado y revoque su derecho "Iniciar sesión localmente" (pero asegúrese de que la cuenta Invitado posee el derecho "Acceder a esta computadora desde la red").

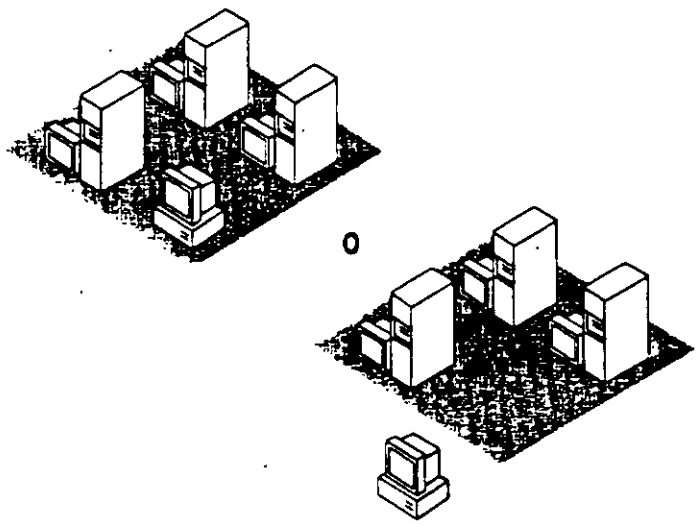
La administración de inicios de sesión de invitados en una estación de trabajo con Windows NT se realiza de la misma manera, excepto que la cuenta esté activada de forma predeterminada, por lo tanto no es necesario realizar una operación si desea permitir inicios de sesión de invitados. De lo contrario, debe desactivar la cuenta Invitado.

Interacción de un dominio con otras computadoras (ordenadores)

En las secciones siguientes se describe la interacción entre un Windows NT Advanced Server de un dominio y otras computadoras existentes en la red.

Interacción con estaciones de trabajo con Windows NT

Recuerde que las estaciones de trabajo con Windows NT pueden formar parte de un dominio y utilizar cuentas de usuarios y grupos globales de ese dominio, y de los dominios en que confíe; o pueden estar aisladas de todos los dominios y usar solamente sus propios usuarios y grupos.



Una estación de trabajo con Windows NT que esté aislada de todos los dominios no tendrá interacción alguna con ningún dominio. Es posible crear grupos locales y cuentas de usuario en la propia estación de trabajo, pero estos serán los únicos usuarios y grupos que podrán utilizarse en la misma. La estación de trabajo no podrá utilizar ninguna cuenta de usuario ni grupo local desde ningún dominio. Un usuario que haya iniciado una sesión utilizando una cuenta de estación de trabajo local no podrá acceder a ningún servidor con Windows NT Advanced Server, excepto si inicia su sesión como invitado.

En una estación de trabajo con Windows NT que forme parte de un dominio, un usuario podrá iniciar sesiones con cuentas de usuario situadas en el dominio de su estación de trabajo (o en cualquier dominio de su confianza). Por ejemplo, supongamos que una estación de trabajo forma parte del dominio Ventas, el cual confía en el dominio Informática. En la estación de trabajo, un usuario podrá iniciar una sesión con una cuenta situada tanto en el dominio Ventas como en Informática.

En una estación de trabajo con Windows NT que forme parte de un dominio, podrán incluirse usuarios y grupos globales del dominio (y de los dominios de su confianza) en grupos locales de la estación de trabajo, así como asignar permisos y derechos sobre la estación de trabajo a usuarios y grupos globales del dominio al que ésta pertenece (y de los dominios de su confianza).

Aunque una estación de trabajo perteneciente a un dominio podrá utilizar las cuentas situadas en el mismo, seguirá siendo posible crear cuentas de usuario en la propia estación de trabajo. Estas cuentas serán locales a esa estación de trabajo y no podrán emplearse en ninguna otra computadora (ordenador). Una posible aplicación de esta técnica es el caso en que un empleado desee crear una cuenta para su cónyuge, con el fin de permitirle la utilización de su procesador de texto fuera de horas de oficina o para compartir los archivos de la estación de trabajo con otros usuarios que no posean una cuenta en el dominio.

Sin embargo, en la estación de trabajo local no debe crearse ninguna cuenta para ningún usuario que ya posea una cuenta en el dominio. Si un usuario posee una cuenta en el dominio, es preferible que inicie siempre las sesiones utilizando dicha cuenta.

Obsérvese que, incluso aunque una estación de trabajo con Windows NT forme parte de un dominio, no podrá utilizar los grupos locales definidos en el mismo (sin embargo, sí podrá utilizar los usuarios y grupos globales definidos en el dominio).

Interacción con servidores ejecutando otros sistemas de red

Con la excepción de los servidores LAN Manager 2.x, los servidores que utilicen sistemas operativos de red distintos de Windows NT Advanced Server (como Novell NetWare o IBM LAN Server) no podrán formar parte de dominios ni compartir información de cuentas con un servidor con Windows NT Advanced Server.

Existen dos formas de incorporar servidores con LAN Manager 2.x a la red:

- Como servidores de un dominio con Windows NT Advanced Server (en el cual el controlador de dominio debe ser un servidor con Windows NT Advanced Server)
- Como partes de dominios con LAN Manager 2.x, en los cuales un servidor con LAN Manager 2.x actúe como controlador de dominio

La incorporación de un servidor con LAN Manager 2.x a un dominio con Windows NT Advanced Server plantea algunos problemas, ya que el servidor con LAN Manager 2.x presenta ciertas limitaciones. Aunque el servidor con LAN Manager 2.x reciba una copia de la base de datos de grupos y usuarios del dominio, no podrá reconocer los grupos locales, por lo que no será posible asignar a los grupos locales del dominio ninguno de los permisos que se aplican a los recursos de los servidores con LAN Manager 2.x.

Asimismo, si el dominio que contiene servidores con LAN Manager 2.x confía en otros dominios, no será posible asignar permisos relativos a los servidores con LAN Manager 2.x a los usuarios y grupos locales del dominio de confianza. Estos servidores no reconocen las relaciones de confianza.

Los dominios constituidos exclusivamente por servidores con LAN Manager 2.x no pueden tener relaciones de confianza con otros dominios, aunque los usuarios de las estaciones de trabajo con Windows NT sí podrán tener acceso a los recursos de dichos dominios. Puesto que los dominios con LAN Manager 2.x no pueden confiar en otros dominios, tampoco pueden utilizar los grupos globales ni los usuarios definidos en otros dominios. Por consiguiente, para que un usuario de Windows NT pueda obtener acceso a un recurso situado en un dominio con LAN Manager 2.x, deberá disponer también de una cuenta en dicho dominio (o ese dominio deberá permitir los inicios de sesión como invitado).

Si desea obtener más información sobre la manera de proporcionar acceso al Windows NT Advanced Server a los usuarios que no dispongan de cuentas Windows NT Advanced Server (pero sí posean cuentas en servidores basados en otros tipos de software de red), consulte la sección "Concepto de cuenta local", más adelante en este mismo capítulo.

Interacción con computadoras (ordenadores) con Windows para Trabajo en grupo

Si dispone de estaciones de trabajo que ejecuten Windows para Trabajo en grupo, éstas interactuarán con las computadoras con Windows NT y Windows NT Advanced Server del mismo modo que las estaciones de trabajo con Windows 3.1 o MS-DOS.

Análogamente, los usuarios de estaciones de trabajo con Windows NT podrán tener acceso a los recursos compartidos en las estaciones de trabajo con Windows para Trabajo en grupo, del mismo modo que cualquier otro usuario de Windows para Trabajo en grupo.

En Windows para Trabajo en grupo, las computadoras están organizadas en *grupos de trabajo*. Los grupos de trabajo son similares a los dominios en lo que se refiere al examen de la red: cuando un usuario emplee el Administrador de archivos para examinar la red, la verá dividida en dominios y grupos de trabajo. Si el usuario selecciona un dominio o grupo de trabajo, podrá examinar el contenido del mismo.

Los dominios y grupos de trabajo pueden interactuar mutuamente. A efectos de examen de la red, los dominios y los grupos de trabajo se comportan del mismo modo. Si una estación de trabajo con Windows NT no forma parte de un dominio, bastará con integrarla en un grupo de trabajo para que pueda ser examinada como parte del mismo. Ese grupo de trabajo podrá incluir computadoras que utilicen Windows para Trabajo en grupo. Análogamente, en una computadora con Windows para Trabajo en grupo, podrá especificarse el nombre de un dominio que ejecuta Windows NT Advanced Server como grupo de trabajo de la computadora, con lo cual la computadora con Windows para Trabajo en grupo podrá aparecer como parte en ese dominio.

Obsérvese que, para que una computadora con Windows para Trabajo en grupo pueda examinar un dominio que ejecuta Windows NT Advanced Server, deberá existir al menos una computadora con Windows para Trabajo en grupo en el dominio que se desee examinar. Si un usuario de Windows para Trabajo en grupo desea obtener acceso a un recurso situado en un dominio en el cual no exista ninguna computadora con Windows para Trabajo en grupo, dicho usuario deberá conocer el nombre de la computadora donde esté situado ese recurso.

Cada vez que se inicie una computadora con Windows para Trabajo en grupo, el usuario será conectado a la red, utilizando un nombre de usuario y una contraseña previamente especificados en la computadora. Si un usuario de Windows para Trabajo en grupo posee una cuenta en un dominio que ejecuta Windows NT Advanced Server, el nombre de usuario y la contraseña de esa cuenta podrán proporcionarse a Windows para Trabajo en grupo, y configurar como nombre del grupo de trabajo en la computadora el nombre del dominio. De este modo, el usuario iniciará automáticamente la sesión con su cuenta de dominio cuando se inicie Windows para Trabajo en grupo.

Concepto de cuenta local

Si en su red existen actualmente servidores con sistemas operativos de red distintos de Windows NT, como LAN Manager 2.x, Novell NetWare o IBM LAN Server, podrá utilizar *cuentas de usuario locales* (o simplemente *cuentas locales*) para facilitar en cierta medida el acceso a través de la red a los distintos usuarios de estos sistemas y a los usuarios que dispongan de cuentas en un dominio que ejecuta Windows NT Advanced Server.

Un cuenta local es una cuenta de usuario cuyo comportamiento es distinto del de las cuentas de usuario normales (también conocidas como *cuentas globales*). Las cuentas locales no pueden utilizarse para iniciar una sesión de forma interactiva en una estación de trabajo con Windows NT o en un servidor con Windows NT Advanced Server, pero en muchos otros aspectos son prácticamente como cualquier otra cuenta de usuario: permiten obtener acceso a computadoras (ordenadores) con Windows NT y Windows NT Advanced Server a través de la red, pueden incluirse en grupos locales y globales, y pueden recibir derechos y permisos de archivos. La única excepción es que las cuentas locales que hayan sido creadas en un dominio no podrán utilizarse en otros dominios que confíen en el suyo. El empleo de cada cuenta local estará limitado a un solo dominio.

Cuando utilice el Administrador de usuarios y el Administrador de archivos, podrá observar, a la izquierda, un icono que indica que se trata de una cuenta local, en lugar del icono estándar de cuenta de usuario.

Existen dos situaciones en las que deberán crearse y emplearse cuentas locales dentro de un dominio: cuando se desee permitir a los usuarios de otros dominios que ejecutan Windows NT Advanced Server, el acceso a los servidores con LAN Manager 2.x de este dominio; y cuando se desee permitir el acceso a aquellos usuarios cuyas cuentas de origen se encuentren en dominios en los cuales no se confíe, o en dominios que ejecutan Windows NT Advanced Server. Estas situaciones se describen con mayor detalle en las siguientes secciones.

Permisos otorgados a los usuarios de Windows NT para el acceso a servidores con LAN Manager 2.x

El sistema de autentificación transparente que utiliza el Windows NT Advanced Server se basa en el hecho de que las relaciones de confianza permiten a los servidores de un dominio reconocer las cuentas de usuario de otros dominios. Sin embargo, incluso aunque los servidores con LAN Manager 2.x pueden formar parte de dominios que ejecuta Windows NT Advanced Server y reconocer las cuentas de usuario en su propio dominio, no pueden reconocer cuentas de usuario procedentes de dominios de su confianza. Esta es una limitación inherente a LAN Manager 2.x.

Por ejemplo, supongamos que el dominio Ventas confía en el dominio Informes. Ello permite asignar permisos a los usuarios de Informes sobre los servidores con Windows NT Advanced Server de Ventas. Sin embargo, no será posible asignar permisos a los usuarios de Informes para los recursos de los servidores con LAN Manager 2.x de Ventas.

Para resolver este problema pueden crearse cuentas locales en el dominio que contiene los servidores con LAN Manager 2.x. Deberá crearse una cuenta local para cada uno de los usuarios de algún dominio de confianza que necesiten obtener acceso a dichos servidores. Las cuentas locales se crean del mismo modo que las cuentas de usuario normales, excepto en que en el momento de crearlas se utilizará el Administrador de usuarios para dominios para designarlas como cuentas locales.

Posteriormente podrá incluir esa cuenta local en grupos globales de su dominio y asignar a dichos grupos globales los permisos necesarios en los servidores con LAN Manager 2.x (para ello deberá utilizar grupos globales, porque los servidores con LAN Manager 2.x no reconocen grupos locales). Aunque puede otorgar permisos directamente a las cuentas locales, no es recomendable hacerlo, ya que ello dificultaría su mantenimiento cuando se decidiera actualizar los servidores con LAN Manager 2.x sustituyéndolos por Windows NT y se dejara de necesitar el empleo de cuentas locales.

Si sustituye todos los servidores de su dominio por servidores con Windows NT Advanced Server, de tal modo que no quede ningún servidor con LAN Manager 2.x, podrá eliminar todas las cuentas locales del dominio y comenzar a referirse en su lugar a las cuentas de Windows NT Advanced Server de dichos usuarios. Cuando llegue el momento de eliminar las cuentas locales de un dominio, el hecho de que sus iconos sean diferentes le ayudará a realizar esta operación de un modo preciso y rápido.

Permisos otorgados a los usuarios de otros sistemas para el acceso a Windows NT

A medida que empiece a agregar a su red servidores con Windows NT Advanced Server y estaciones de trabajo con Windows NT, puede producirse el caso en que algunas cuentas de usuario se encuentren en dominios con Windows NT Advanced Server, mientras que otras estén situadas en servidores de otros sistemas, como LAN Manager 2.x, Novell NetWare o IBM LAN Server.

Para permitir a los usuarios que tengan cuenta en otros sistemas el acceso a los recursos de Windows NT, puede crear cuentas locales para aquellos usuarios de los dominios con Windows NT Advanced Server que contengan dichos recursos. Posteriormente podrá incluir esas cuentas en grupos locales del dominio y asignar a esos grupos locales los permisos necesarios. Aunque es posible otorgar permisos directamente a las cuentas locales, no se recomienda hacerlo, ya que ello dificultaría el mantenimiento en caso de que más adelante se decidiera sustituir aquellos sistemas por Windows NT Advanced Server y dejara de ser necesario el empleo de cuentas locales.

Si decide realmente sustituir otros sistemas por Windows NT después de haber otorgado cuentas locales a sus usuarios, podrá eliminar las cuentas locales y empezar a utilizar para esos usuarios las cuentas de Windows NT Advanced Server.

Las cuentas locales se diferencian de otras cuentas de usuario en un aspecto muy importante: una cuenta local de un dominio no puede utilizarse en dominios que confíen en él. Por lo tanto, si un usuario de otro sistema operativo de red necesita obtener acceso a varios dominios que ejecutan Windows NT Advanced Server, deberá crear una cuenta local para dicho usuario en cada uno de esos dominios Windows NT.

Protección contra virus y caballos de Troya

En el mundo informático actual, es necesario impedir intrusiones malintencionadas en la red, que se manifiestan en forma de virus o caballos de Troya. Los *virus* son programas que intentan esparcirse de una computadora a otra y provocar algún tipo de daño (destruyendo o alterando datos) o molestias a los usuarios (imprimiendo mensajes o alterando lo que aparece en pantalla) en todas las computadoras con las cuales entran en contacto. Los *caballos de Troya* son programas que se enmascaran bajo el aspecto de otros programas comunes, en un intento por capturar información. Un ejemplo de caballo de Troya es un programa que se oculta bajo el aspecto de una pantalla de inicio de sesión del sistema e intenta capturar la información de nombres de usuarios y contraseñas, información que los autores del caballo de Troya podrán utilizar posteriormente para entrar en el sistema. Es posible protegerse en gran medida contra los ataques de virus y caballos de Troya con sólo realizar unas sencillas operaciones.

Prevención contra infecciones de virus

Es poco probable que alguno de los usuarios de su red desarrolle un virus y lo introduzca en el sistema. Es mucho más probable que algún usuario introduzca inadvertidamente un virus en su red creyendo utilizar un programa seguro y útil procedente de alguna otra fuente, como un boletín electrónico. La mayoría de los usuarios de la red no son conscientes de que pueden introducir los virus en la red de esta manera, por lo que una de las mejores formas de mantener la seguridad de la red impidiendo el acceso de virus es educar a los usuarios acerca de los mismos.

También conviene disponer de al menos un programa comercial de detección de virus y utilizarlo con regularidad para comprobar si existe algún virus en los servidores de archivos. Si es posible, deberá poner el software de detección de virus a disposición de sus usuarios.

He aquí otras maneras de protegerse contra los virus:

- Establecer permisos de archivos de tal modo que todas las aplicaciones disponibles en los servidores de red y en las estaciones de trabajo con Windows NT sólo puedan leerse y ejecutarse, para evitar que puedan ser sustituidas por virus. Si desea obtener más información en este sentido, consulte el capítulo 5, "Administración de archivos de la red".
- Antes de introducir una nueva aplicación o archivo en la red, cópielo en una computadora (ordenador) que no esté conectada a la red y aplíquele el software de detección de virus. También puede iniciar una sesión en esta computadora utilizando una cuenta cuyo nivel de acceso a la computadora sea únicamente el de Invitado, a fin de que el programa sometido a verificación sólo posea los permisos correspondientes a esta categoría y no sea capaz de modificar ningún archivo importante.
- Realice periódicamente copias de seguridad de los archivos de los servidores (y de las estaciones de trabajo, si es posible), a fin de reducir al mínimo el daño en caso de que llegue a producirse el ataque de un virus. Si desea obtener más información sobre las copias de seguridad, consulte el capítulo 8, "Copia de seguridad de archivos de red".

Prevención contra ataques de caballos de Troya

Windows NT ofrece una importante medida de seguridad contra los programas conocidos como caballos de Troya: para que un usuario pueda iniciar una sesión en una estación de trabajo con Windows NT o en un Windows NT Advanced Server, deberá introducir la *secuencia protegida de atención*, CTRL+ALT+SUPR. Esta serie de teclas invoca directamente la pantalla de inicio de sesión del sistema operativo Windows NT. Los caballos de Troya nunca podrán entran en acción si se utiliza este procedimiento. De este modo, se garantiza que los usuarios sólo proporcionen su nombre de usuario y su contraseña al propio sistema operativo. Para garantizar la eficacia de este método, es necesario educar a los usuarios para que siempre presionen CTRL+ALT+SUPR antes de iniciar una sesión en una computadora, incluso aunque ya aparezca en la pantalla la ventana de inicio de sesión.

La secuencia protegida de atención también es necesaria para que un usuario pueda desbloquear una estación de trabajo bloqueada o cambiar su contraseña.

La otra forma de impedir los caballos de Troya es idéntica al método de protección contra virus: convertir todas las aplicaciones en archivos que sólo puedan leerse y ejecutarse, a fin de que no puedan ser sustituidos por ningún programa que se oculte bajo la apariencia del programa original y usurpe información.

Ejemplos de seguridad de red

En las secciones siguientes se ofrecen algunos ejemplos que ilustran los distintos métodos que pueden utilizarse para aplicar los conceptos descritos en este capítulo.

Uso del modelo de dominio maestro

Una empresa de 3.000 usuarios, dividida en 15 departamentos y una administración de sistema de información (MIS) centralizado, está configurando su red de Windows NT Advanced Server. La empresa ha seleccionado como modelo de seguridad de Windows NT Advanced Server el modelo de dominio maestro.

El grupo MIS creará un dominio con el nombre MIS, que actuará como dominio maestro. Este dominio posee 3 servidores que ejecutan Windows NT Advanced Server, lo cual permite garantizar el funcionamiento de la red en caso de que falle alguno de los servidores.

Todas las cuentas de usuario se crean en el dominio MIS. El grupo MIS ha creado además 15 grupos globales en el dominio MIS. El nombre de cada uno de estos grupos globales se corresponde con el de uno de los 15 departamentos de la empresa. Los miembros de cada grupo global son los empleados que trabajan en el departamento respectivo. Inicialmente, cada empleado sólo es miembro de uno de estos grupos globales. En el dominio MIS no se comparte ningún directorio ni impresora; este dominio se utiliza únicamente para la administración de cuentas.

Cada uno de los 15 departamentos posee su propio dominio que ejecuta Windows NT Advanced Server. La mayoría de estos dominios departamentales contiene un solo servidor con Windows NT Advanced Server. Todos los directorios e impresoras de la red son compartidos dentro de los dominios departamentales. Todos y cada uno de los dominios departamentales confían en el dominio MIS, pero ninguno de dichos departamentos necesita confiar en los otros.

El grupo local Administradores de cada uno de los dominios departamentales contiene la cuenta de usuario de al menos un usuario que trabaje en ese departamento, a fin de que dicho usuario pueda compartir directorios y crear grupos locales en el dominio, así como realizar otras tareas necesarias. El grupo "MIS\Administradores de dominios" es miembro también del grupo local Administradores de cada uno de los dominios, a fin de que el grupo MIS pueda realizar actualizaciones de software, copias de seguridad de los servidores de red y proporcionar ayuda a los administradores departamentales en caso de que se produzca algún problema de difícil solución. (Si lo desea, podría especificar que los directores departamentales sean únicamente Operadores de servidores dentro de sus propios dominios. De este modo, podrán compartir recursos, pero la creación de grupos locales y otras tareas administrativas se dejará a la exclusiva responsabilidad del grupo MIS.)

Cuando un administrador de un departamento local necesite crear una nueva agrupación de usuarios que vaya a ser utilizada únicamente en ese dominio, podrá crear un grupo local dentro del dominio. Por ejemplo, el administrador del dominio Ventas podrá crear un nuevo grupo local dentro del dominio Ventas, con las cuentas de usuario MIS\CarlosM, MIS\MaríaB y MIS\PedroE. En este ejemplo, CarlosM, MaríaB y PedroE trabajan en el dominio Ventas, pero al igual que todos los demás empleados de la empresa, sus cuentas están localizadas de forma centralizada en el dominio MIS.

Supongamos que es necesario establecer una nueva agrupación de usuarios y que dicho grupo necesita disponer de permisos sobre más de un dominio, o debe incluir usuarios procedentes de varios dominios diferentes. En este caso, el administrador de un departamento local podrá enviar un mensaje al grupo MIS, el cual creará un grupo global dentro del dominio MIS con los miembros adecuados. Por ejemplo, si el grupo MIS crea un grupo global llamado "Planificadores" dentro del dominio MIS, el director de un departamento podrá conceder a "MIS\Planificadores" los permisos requeridos para los recursos que dicho grupo necesite.

Uso del modelo de dominio maestro múltiple

Una empresa en expansión integrada por 20.000 usuarios, divididos en 100 departamentos y un grupo centralizado MIS, está instalando una red de Windows NT Advanced Server. Debido al gran número de usuarios, la empresa selecciona el modelo de dominio maestro múltiple, para que el rendimiento de los dominios maestros no se resienta.

La empresa ha creado 3 dominios maestros (MIS-Desarrollo, MIS-Ventas e MIS-Administración), cada uno de ellos con 6 servidores con Windows NT Advanced Server. El número relativamente elevado de servidores en cada dominio ofrece una mayor velocidad en la aprobación de peticiones de inicio de sesión, algo necesario si se tiene en cuenta que a una misma hora de la mañana pueden estar iniciando una sesión un gran número de empleados a la vez. La empresa ha optado por utilizar 3 dominios maestros, en lugar de usar únicamente 2, para permitir que el modelo actual pueda acomodarse al crecimiento progresivo de la empresa.

Todas las cuentas de usuario se crean en uno de los dominios MIS. El dominio maestro en el cual estará englobada la cuenta del usuario dependerá del trabajo que éste realice. Por ejemplo, las cuentas de todos los usuarios que trabajen en el desarrollo de productos se encontrarán en MIS-Desarrollo.

Cada uno de los departamentos individuales posee su propio dominio con su propio administrador, el cual se encarga de crear grupos locales, administrar la compartición de los recursos departamentales y mantener en funcionamiento los servidores de los departamentos.

Cada uno de los 3 dominios maestros confía en los otros, del mismo modo que cada uno de los dominios departamentales confía en todos los dominios maestros. Los dominios departamentales no necesitan confiar entre sí.

Si se necesita establecer una nueva agrupación global de usuarios, ésta deberá ser creada por el grupo MIS. Si es necesario que el grupo global contenga usuarios procedentes de dos de los dominios maestros de la red, en realidad el grupo MIS necesitará crear dos grupos globales, uno en cada dominio maestro, que contendrán los usuarios cuyas cuentas se encuentren en ese dominio. Por ejemplo, un grupo que contenga usuarios tanto de MIS-Ventas como de MIS-Administración puede necesitar examinar los informes de ventas anuales. Para ello puede crear grupos con los nombres "Informes de ventas" en cada uno de estos dominios. Posteriormente, cuando asigne los permisos, deberá asegurarse de asignarlos tanto a "MIS-Ventas\Informes de ventas" como a "MIS-Administración\Informes de ventas".

Uso del modelo de confianza total

Una empresa de 1.000 usuarios sin grupo centralizado de MIS está configurando su red de Windows NT Advanced Server. Puesto que no existe una administración informática centralizada, cada departamento tendrá que administrar sus propios servidores. Por tanto, la opción más indicada es el modelo de confianza total.

Cada departamento configurará su propio dominio y tendrá su propio Administrador del dominio, que será responsable absoluto tanto de las cuentas de usuario como de los recursos compartidos del dominio. Cada uno de los administradores del dominio creará cuentas de usuario para todos los empleados que trabajen en el departamento correspondiente a ese dominio.

Cada uno de los administradores departamentales será también responsable de crear grupos globales y grupos locales en su dominio. Cuando el administrador departamental cree un grupo que incluya únicamente usuarios de ese dominio departamental, podrá crear un grupo global. Cuando sea necesario que un grupo contenga usuarios de otros dominios, será preciso crear un grupo local.

Cada administrador departamental podrá establecer relaciones de confianza bidireccionales con otros dominios de Windows NT Advanced Server. Los usuarios y grupos globales de un dominio podrán recibir derechos y permisos, o incluirse en grupos locales, en el otro dominio.

En este caso, los administradores departamentales tendrán la responsabilidad de garantizar que sólo se incorporen a los grupos globales las personas adecuadas. Por ejemplo, si el departamento Transportes confía en el departamento Ventas, el administrador de Transportes podrá otorgar permisos al grupo global Contables del dominio Ventas. Si el administrador de Ventas añade posteriormente más usuarios al grupo global Contables, esos nuevos usuarios adquirirán inmediatamente los permisos que hayan sido concedidos a Contables en el dominio Transportes. Por tanto, el administrador de Transportes deberá tener cuidado de conceder permisos únicamente a los grupos globales adecuados de los dominios con administradores de su confianza, y el administrador de Ventas será responsable de incluir en los grupos globales únicamente usuarios adecuados.

Uso de los grupos locales de operadores

Supongamos que un grupo de mediano tamaño está intentando decidir cómo asignar su personal técnico a los distintos grupos de operadores y administradores.

Por lo menos una persona debe ser administrador. Existen diversas facultades de gran importancia que sólo están a disposición de los administradores, como la asignación de derechos de usuario, la toma de posesión de archivos y la administración de la auditoría. Dadas las características únicas del grupo Administradores, los miembros de este grupo son responsables absolutos de la planificación y mantenimiento de la seguridad de la red en el departamento. También es posible permitir a los miembros del grupo "Administradores de dominios" que administren las estaciones de trabajo con Windows NT de los usuarios, si se desea.

Si alguien del grupo es responsable de contratar nuevos empleados o trabajadores temporales, o simplemente si hay alguien responsable de ayudar a los recién llegados a familiarizarse con el sistema, tiene sentido que esta persona sea miembro del grupo Operadores de cuentas. Este operador de cuentas podrá crear cuentas en el dominio para la formación de los nuevos empleados e incluir dichas cuentas en los grupos adecuados.

Si el grupo "Administradores de dominios" tiene pocos miembros, probablemente interesará asignar al menos una persona adicional al grupo Operadores de servidores. La función básica de los miembros del grupo Operadores de servidores es mantener en funcionamiento los servidores del dominio. Esta misión queda reflejada en sus facultades, que incluyen la posibilidad de apagar servidores, ajustar la hora del sistema en los servidores, bloquear y saltarse el bloqueo de los servidores, compartir directorios e impresoras en el servidor, y formatear su disco duro. Si es posible, conviene asegurarse de que al menos un miembro de los grupos Administradores u Operadores de servidores esté presente durante todas las horas en que alguien esté utilizando la red.

Si la posibilidad de imprimir documentos rápidamente es muy importante para su grupo, puede ser conveniente incluir en el grupo "Operadores de impresión" a varias personas capacitadas para este puesto, a fin de garantizar que los problemas relacionados con la impresora sean resueltos rápidamente en cualquier momento.

Configuración de un grupo de operadores universal

Supongamos que una red contiene múltiples dominios, en cada uno de los cuales existen sistemas de cuyo contenido es necesario realizar copias de seguridad. Se dispone de un solo grupo de operadores de copia de seguridad y se desea que dicho grupo pueda realizar copias de seguridad de las computadoras (ordenadores) de todos los dominios.

Para establecer esta configuración deberá utilizarse una combinación de grupos locales y globales. Con ello se garantizará que el grupo de operadores de copia de seguridad resulte fácil de mantener a medida que se amplíe la red y vayan rotando los operadores de copia de seguridad, vayan incorporándose nuevas computadoras o incluso se añadan nuevos dominios.

1. En cada uno de los dominios en los cuales estén situadas las cuentas de los operadores de copia de seguridad, cree un grupo local llamado "Operadores de copia de seguridad del dominio" y convierta a todos los operadores de copia de seguridad del dominio en miembros de ese grupo.
2. En cada uno de los dominios en los cuales sea necesario realizar copias de seguridad, incluya todos los grupos globales "Operadores de copia de seguridad del dominio" en el grupo local "Operadores de copia de seguridad" del dominio local. Cuando lo haga, no olvide de incluir el grupo global "Operadores del copia de seguridad del dominio" de cada uno de los dominios en el propio grupo local "Operadores de copia de seguridad" de ese dominio.

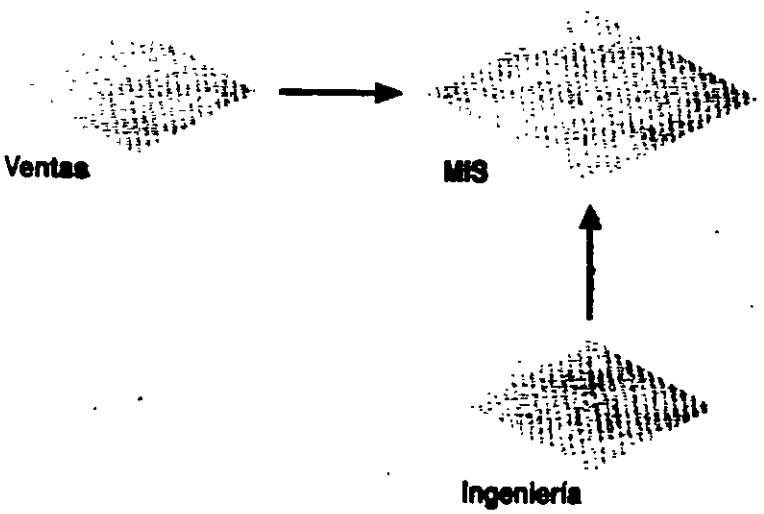
Una vez lo haya hecho, todos los operadores de copia de seguridad podrán realizar copias de seguridad en todas las computadoras necesarias.

Si necesita también efectuar copias de seguridad de las estaciones de trabajo con Windows NT, deberá realizar una operación adicional, ya que las estaciones de trabajo con Windows NT no pueden utilizar los grupos locales de un dominio (por ejemplo, Operadores de copia de seguridad), incluso aunque dichas estaciones de trabajo formen parte de ese dominio.

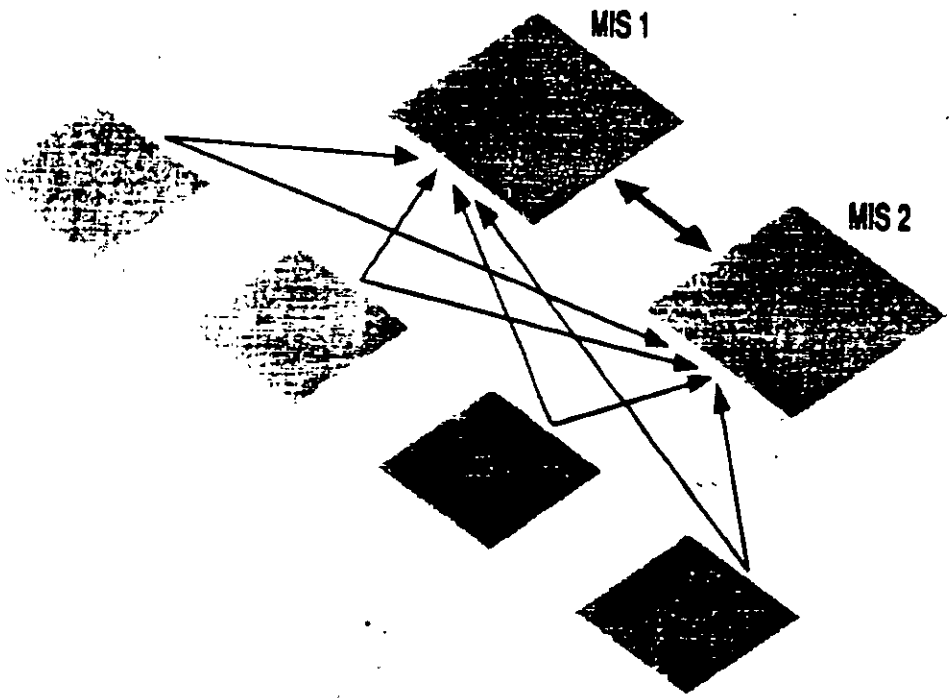
Para permitir esta posibilidad, en cada una de las estaciones de trabajo con Windows NT de las que se necesite realizar copia de seguridad, incorpore todos los grupos globales "Operadores de copia de seguridad del dominio" al grupo local "Operadores de copia de seguridad" de la estación de trabajo.

El mantenimiento de este modelo es muy sencillo. Si un operador de copia de seguridad abandona la empresa, o llega uno nuevo, bastará con eliminar o incorporar la cuenta de ese usuario al grupo global "Operadores de copia de seguridad del dominio" correspondiente al dominio en el cual esté situada la cuenta del usuario. Si se añaden a un dominio existente nuevos servidores de los cuales se necesite realizar copias de seguridad, todos sus operadores de copia de seguridad podrán encargarse de ello automáticamente. Si necesita realizar copias de seguridad en otra estación de trabajo, bastará con que incorpore todos los grupos globales "Operadores de copia de seguridad del dominio" al grupo local "Operadores de copia de seguridad" de la estación de trabajo. Si incorpora un nuevo dominio a su red, bastará con que agregue todos los grupos globales "Operadores de copia de seguridad del dominio" al grupo local "Operadores de copia de seguridad" de ese nuevo dominio.

Por ejemplo, supongamos que tenemos la configuración de red que se muestra en la figura siguiente, en la que se utiliza el modelo de dominio maestro, donde MIS es el dominio maestro.



Puesto que MIS es el único dominio maestro, todas las cuentas de usuario estarán situadas allí. Para crear el grupo de operadores universales de copia de seguridad, bastará con crear el grupo global "Operadores de copia de seguridad del dominio" en el dominio MIS e incluir el grupo "MIS\Operadores de copia de seguridad del dominio" en los grupos locales "Operadores de copia de seguridad" de los tres dominios. A continuación, bastará con añadir al grupo global "Operadores de copia de seguridad del dominio" las cuentas de usuario de cada uno de los operadores de copia de seguridad, con lo cual habrá quedado concluida la configuración.



Si el modelo utilizado en la red es el de dominio maestro múltiple, como en la figura, con dos dominios maestros (MIS1 e MIS2), bastará con crear grupos globales de "Operadores de copia de seguridad del dominio" tanto en MIS1 como en MIS2, e incorporar tanto "MIS1\Operadores de copia de seguridad del dominio" como "MIS2\Operadores de copia de seguridad del dominio" al grupo local "Operadores de copia de seguridad" de cada uno de los dominios.

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

DIPLOMADO EN REDES (LAN)

MODULO III

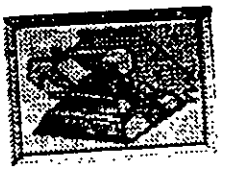
INSTALACION Y MANEJO DE REDES (LAN)

DE MICROS CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

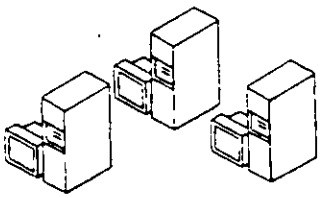
MATERIAL DIDACTICO

MAYO , 1996

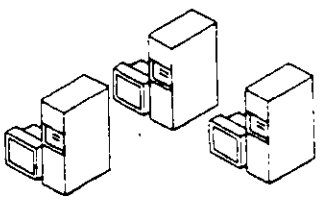
Palacio de Minería Calle de Tacuba 5 Primer piso [illegible] 06000 Mexico D.F. APDO [illegible]
Teléfonos 512-8955 512-5121 521-7335 [illegible] 510 0573 512-5121 521 4020 [illegible]



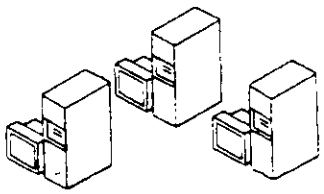
WINDOWS NT DOMINIOS



dominio
Finanzas

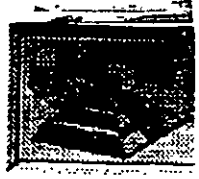


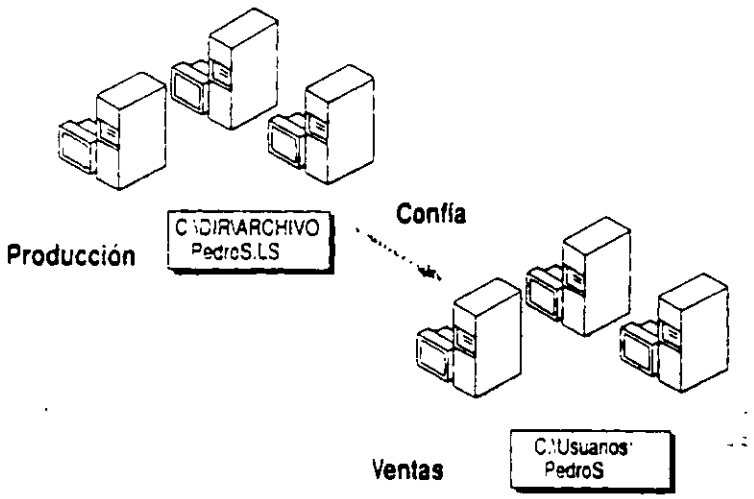
dominio
Producción



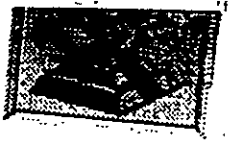
dominio
Ventas

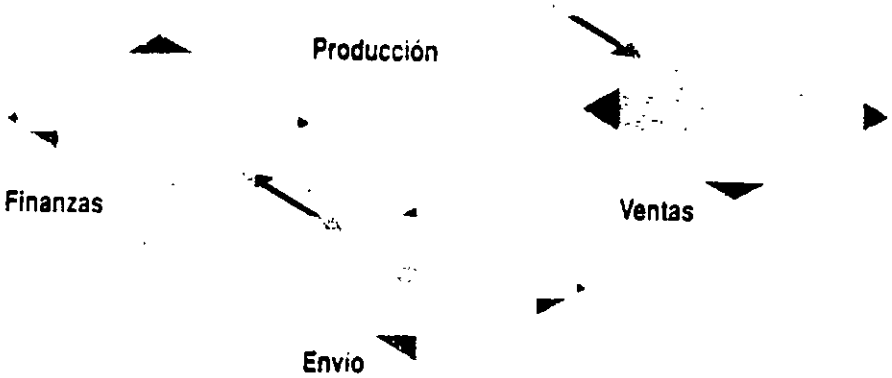
Notas:




Producción
C:\DIR\ARCHIVO
PedroS.LS
Confía
Ventas
C:\Usuarios
PedroS

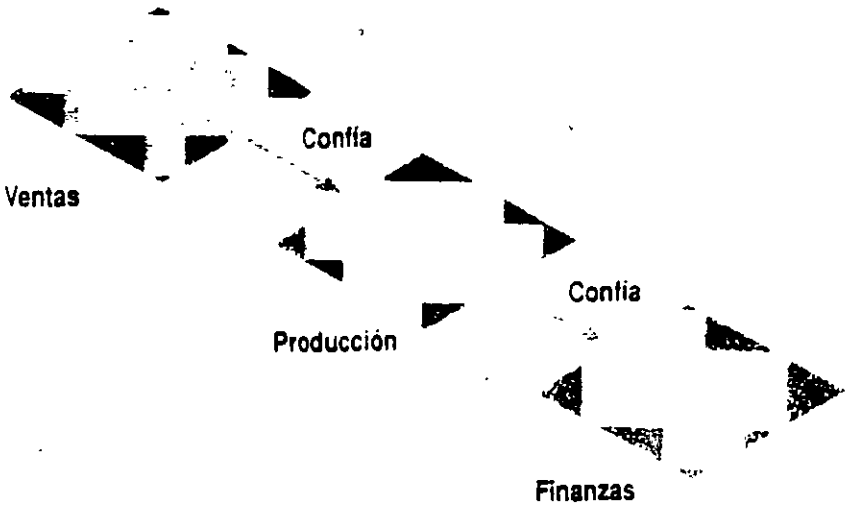
Notas:





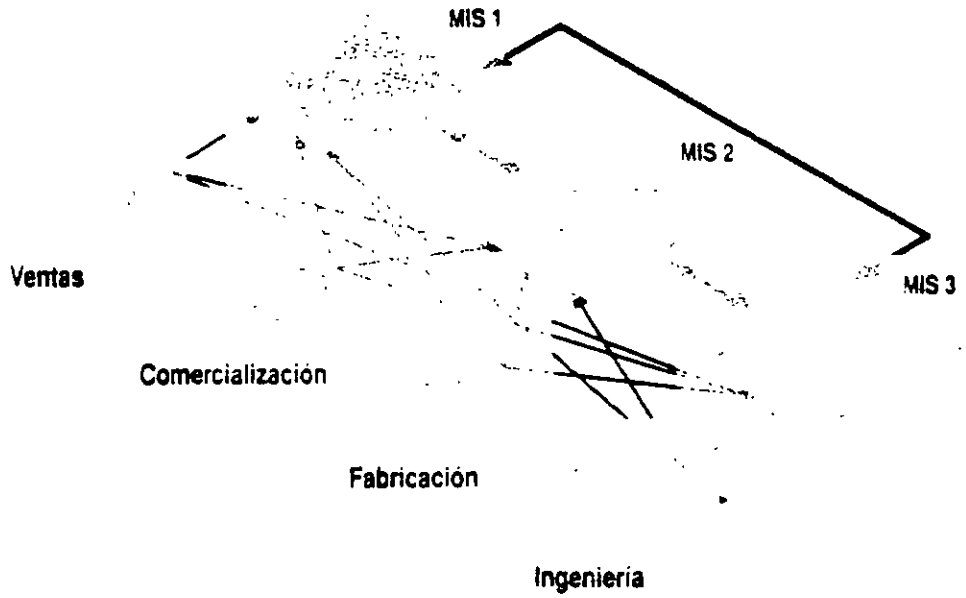
Notas:

WINDOWS NT RELACIONES DE CONFIANZA



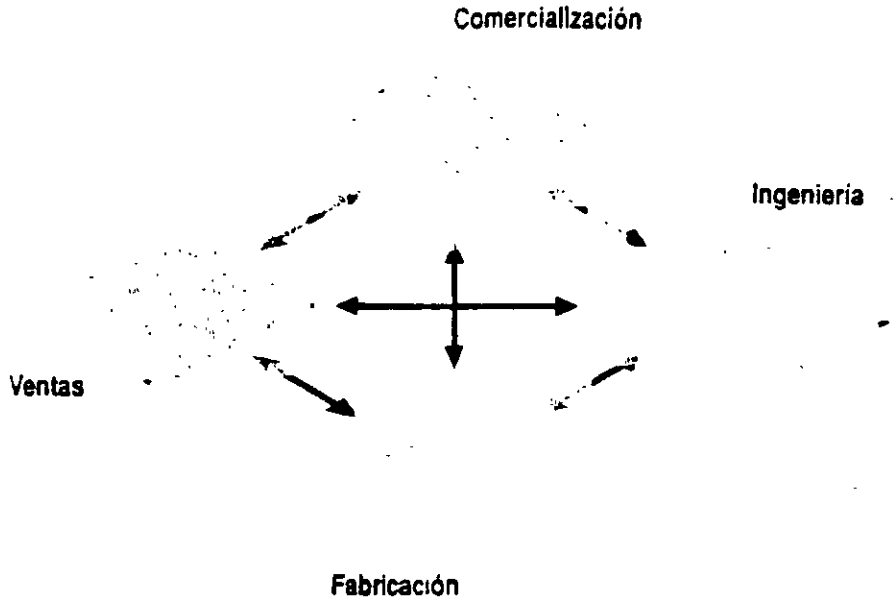
Notas:

WINDOWS NT MODELO DE DOMINIO MAESTRO MULTIPLE



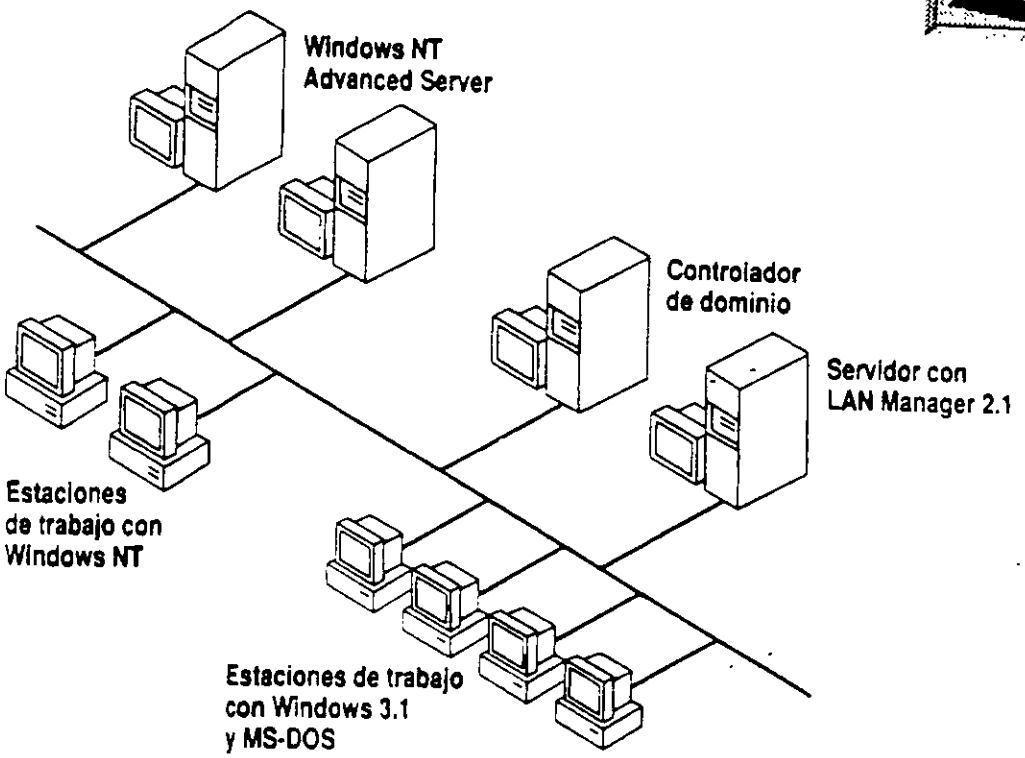
Notas:

WINDOWS NT MODELO DE CONFIANZA TOTAL



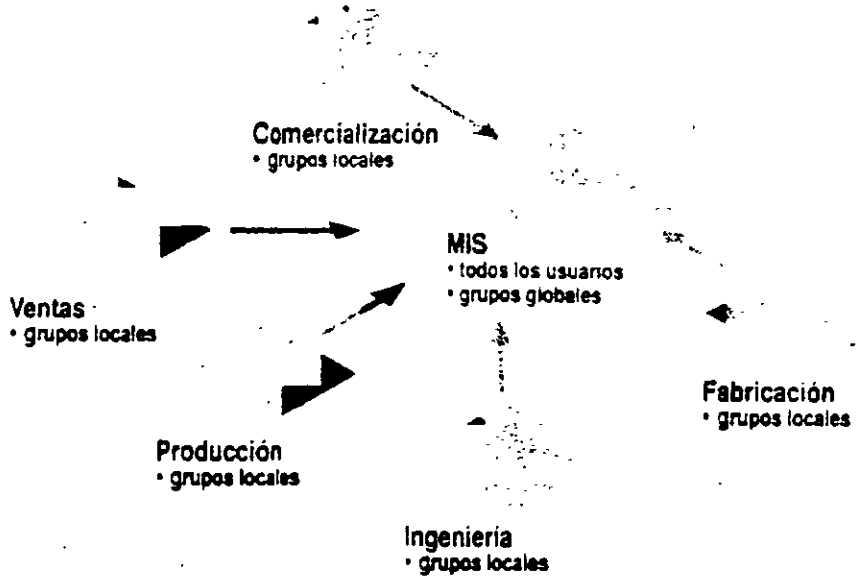
Notas:

WINDOWS NT CONSTITUCION DE UN DOMINIO



Notas:

WINDOWS NT MODELO DE DOMINIO MAESTRO



Notas:

Nombres ARC

Para configurar la información de inicialización para realizar una recuperación en el entorno Windows NT, debe comprenderse el concepto de nombres ARC y cómo se construyen. Los nombres ARC constituyen un método genérico de identificación de dispositivos en el entorno ARC. Para los dispositivos de disco, dichos nombres se construyen del la manera siguiente:

<componente>(x)disk(y)rdisk(z)partition(a)

donde:

<componente> identifica el adaptador de hardware para el dispositivo. Los dos valores válidos para este campo son **scsi** y **multi**, donde **scsi** indica un disco SCSI y **multi** indica una interfaz de disco distinto de SCSI. Para Windows NT, éste podría ser un disco compatible con el controlador AtDisk, o bien con AbiosDsk o CpqArray.

x es el número ordinal del adaptador. Por ejemplo, si hay dos adaptadores SCSI en el sistema, se asignará el ordinal **0** al primero que se cargue e inicialice, y el siguiente número asignado será el **1**. Así sucesivamente para todos los controladores de adaptador que inicialice.

y es, para **scsi**, el número del bus SCSI para adaptadores de bus múltiple SCSI multiplicado por 32 más el identificador de destino del disco. Para **multi**, es siempre **0**.

z es, para **scsi**, el número de unidad lógica. Para **multi**, es el ordinal para el disco en el adaptador.

a es el ordinal de la partición usada en el disco. Todas las particiones reciben un nombre, excepto las particiones tipo 5 (extendida MS-DOS) y 0 (no utilizada).

Por ejemplo, si el árbol de Windows NT se sitúa en la cuarta partición de un disco SCSI con identificador de destino 3 en el segundo controlador SCSI del sistema, el nombre ARC es:

scsi(1)disk(3)rdisk(0)partition(4)

Recuperación de la partición de inicialización

El entorno de inicialización es diferente en las computadoras (ordenadores) tipo x86 y tipo RISC; por lo tanto, los métodos de recuperación de la partición de inicialización también son distintos.

Recuperación en sistemas basados en x86

En computadoras tipo x86, hay un archivo BOOT.INI situado en la partición usada por el BIOS como partición de inicialización. Este archivo contiene selecciones de menú y la situación del nombre ARC en el árbol de inicialización de Windows NT. En este caso, los nombres ARC se construyen de la misma manera que en una computadora tipo RISC. Sin embargo, como el entorno x86 no es ARC, hay un parámetro adicional que utiliza el cargador de inicialización de Windows NT para distinguir entre diversos adaptadores SCSI del mismo tipo.

Por ejemplo, si el sistema contiene un adaptador SCSI Adaptec y dos adaptadores Future Domain SCSI, y la partición de inicialización está situada en el segundo adaptador Future Domain, los nombres ARC serán como sigue:

scsi(0)disk()rdisk()partition() es la base para los dispositivos SCSI Adaptec.

scsi(1)disk()rdisk()partition() es la base para el primer adaptador Future Domain.

scsi(2)disk()rdisk()partition() es la base para el segundo adaptador Future Domain.

A causa de la naturaleza del entorno del cargador de Windows NT, el cargador de inicialización en computadoras (ordenadores) tipo x86 no puede distinguir entre dos adaptadores Future Domain sin información adicional. Dicha información es el ordinal entre los dos adaptadores Future Domain, que se indica al cargador de inicialización a través del parámetro */SCSIORDINAL:n* que se agrega como primera opción de cargador al final de la línea de descripción del nombre ARC en la sección [operating systems] del archivo BOOT.INI. Para este ejemplo, el valor de *n* es **1** (los ordinales comienzan por 0).

En el caso de un espejo de discos de Windows NT Advanced Server para el árbol de inicialización, se crea un disquete de inicialización dándole formato utilizando el sistema operativo Windows NT y copiando en él los siguientes archivos:

- NTLDR
- NTDETECT.COM
- NTBOOTDD.SYS (se requiere solamente si la partición de inicialización está en un disco SCSI; este archivo es el controlador de minipuerto SCSI usado para encontrar el disco espejo)
- BOOT.INI (con una ruta de acceso alternativa que apunte a la copia espejo de la partición del sistema, especificada según las convenciones de nombres ARC)

Recuperación en sistemas basados en RISC

Las computadoras tipo RISC que se ajustan al entorno ARC mantienen la información equivalente para el cargador del sistema operativo en RAM no volátil. Por lo tanto, el proceso de creación de un "disco de inicialización" para las computadoras tipo RISC usando el firmware de Microsoft consiste en la copia de los siguientes archivos en un disco en blanco al que se ha formateado Windows NT:

- OSLOADER.EXE
- HAL.DLL

El firmware de Microsoft ofrece operaciones de mantenimiento de inicialización a través de selecciones en menús. Para configurar una selección de inicialización para el disco de inicialización, establezca el valor de OSLOADER en multi(0)disk(0)fdisk(0)\OSLOADER.EXE y el de SYSTEMPARTITION en multi(0)disk(0)fdisk(0). El valor de fdisk(x) puede cambiarse a 1 para usar el segundo disco del sistema. Si el disco utilizado en el sistema ARC es SCSI, cambie *multi* por *scsi* y siga las reglas para nombres ARC que se citaron previamente para el identificador de destino SCSI.

Después de que el programa Cargador de Windows NT haya finalizado de cargar Windows NT y los controladores configurados, los servicios tolerantes a fallos estarán presentes y podrán realizar las restantes labores correctivas para iniciar el sistema. No obstante, observe que los sistemas RISC pueden acceder solamente a dispositivos SCSI conectados al adaptador SCSI incorporado durante el proceso de inicialización mediante firmware. Por lo tanto, para proteger la partición del sistema o de inicialización en un sistema RISC, ambas unidades deben estar conectadas al adaptador SCSI interno.

Mantenimiento del disco de inicialización

Debe actualizarse el disco de inicialización siempre que se cambien particiones. Por ejemplo, si está usando la partición 2 en la inicialización y elimina la partición 1, deberá cambiar el nombre ARC de manera que en la inicialización se utilice la partición 1. Igualmente, si está usando la partición 2 en la inicialización, y elimina la partición 1 y la reparte entre las particiones 1 y 2, deberá cambiar el nombre ARC de manera que en la inicialización se utilice la partición 3.

Nota Si la partición de inicialización del sistema se encuentra en un disco espejo, es muy recomendable que cree un disco de inicialización mientras el sistema sea operativo. No podrá crear uno mientras el disco principal esté fuera de servicio. El disco de inicialización de tolerancia a fallos debe realizarse a partir de un disco en blanco al que se haya dado formato por medio de Windows NT.

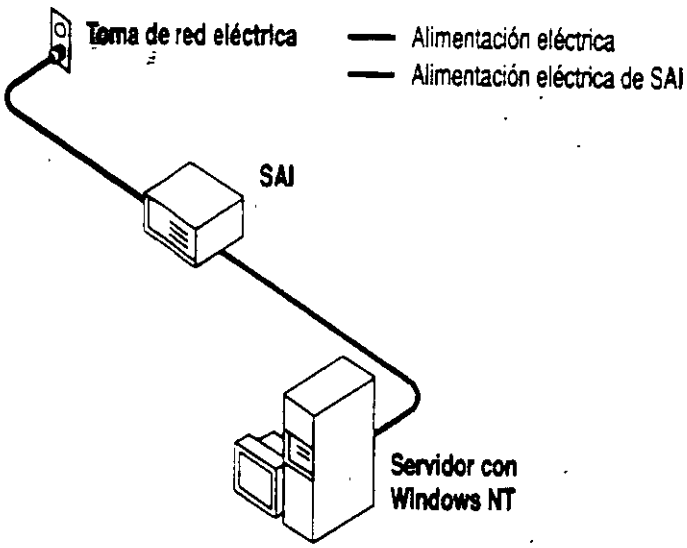
Administración de sistemas de alimentación ininterrumpida

Los sistemas de alimentación ininterrumpida (SAI) proporcionan alimentación cuando hay un corte en el suministro local. Se diseñan normalmente para proporcionar una cantidad determinada de corriente durante un período de tiempo específico. Dicha corriente proviene de pilas que se mantienen cargadas mientras esté disponible la alimentación principal. Esta se convierte de corriente alterna a corriente continua que se utiliza para cargar la pila. Cuando se necesite, la alimentación de corriente continua se convertirá en voltaje de corriente alterna compatible con la fuente de alimentación de la computadora (ordenador). Normalmente, todo lo que se requiere de un SAI es el tiempo necesario para apagar el sistema de forma ordenada terminando los procesos y cerrando las sesiones.

Tipos de SAI

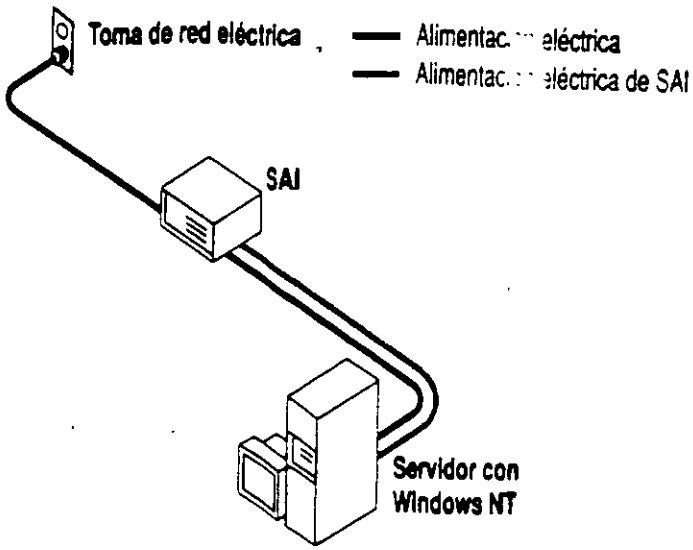
Los sistemas de alimentación ininterrumpida se clasifican en dos categorías: sistemas directo y de reserva.

Un *SAI directo* se conecta entre la alimentación eléctrica y la computadora (ordenador) de manera que suministre constantemente corriente. La conexión a la alimentación eléctrica mantiene cargada su pila. Este método proporciona un *acondicionamiento de corriente*, que significa que se eliminan picos, subidas y caídas de tensión, y ruido.



Configuración de un SAI directo

Un *SAI de reserva* se configura de manera que suministre corriente de la alimentación eléctrica o bien de su propia fuente, y que cambie de una a otra cuando sea necesario. Cuando la alimentación eléctrica está disponible, el dispositivo SAI la conecta directamente a la computadora y supervisa su nivel de tensión. El SAI se mantiene de reserva (es decir, listo para proporcionar corriente pero utilizando muy poca) y la pila se mantiene cargada. Si se produce un corte en la alimentación principal o su voltaje cae por debajo de un nivel aceptable, el dispositivo SAI cambia la alimentación principal por su propia alimentación. Esto debería suceder tan rápidamente que la fuente de alimentación de la computadora proporcionaría un servicio ininterrumpido. Un SAI de reserva puede proporcionar acondicionamiento de corriente durante el servicio normal si está montado en la línea de alimentación principal, pero ésta no es una función del proceso de conversión de la fuente de alimentación del SAI.



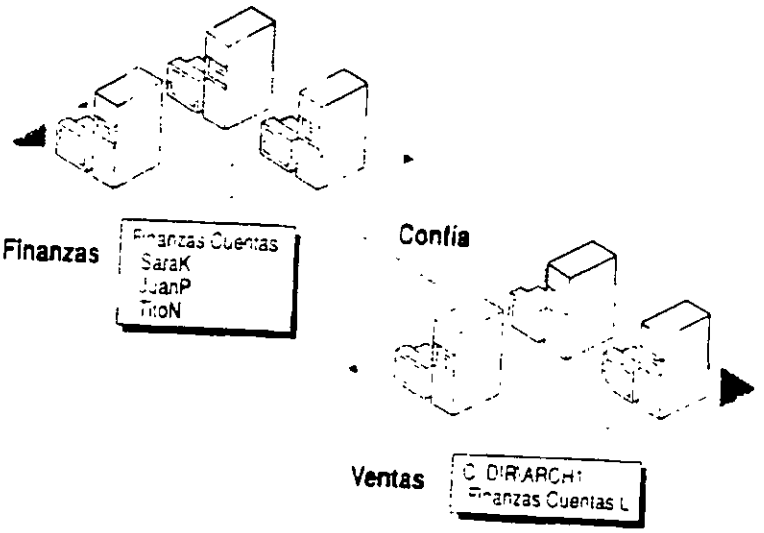
Configuración de un SAI de reserva

También pueden existir versiones híbridas de estos dos tipos. Verifique la seguridad y el mecanismo de tratamiento de fallos del SAI, antes de adquirir o instalar uno.

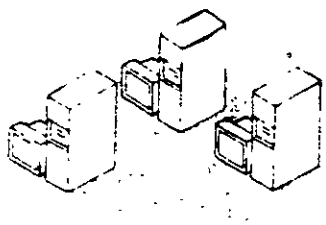
Interacción entre SAI y sistemas operativos

Muchos dispositivos SAI ofrecen la posibilidad de establecer una interfaz con el sistema operativo, permitiendo a éste notificar a los usuarios automáticamente el proceso de apagado, o que la alimentación se ha restaurado y el apagado ya no es necesario.

Durante un corte en la alimentación eléctrica, el servicio de SAI interrumpe inmediatamente el servicio Servidor para evitar cualquier nueva conexión y envía un mensaje para notificar a los usuarios dicho corte de alimentación. El servicio de SAI esperará durante un intervalo de tiempo especificado antes de notificar a los usuarios que deben terminar sus sesiones. Si la alimentación se restaura durante ese intervalo, se enviará otro mensaje informando a los usuarios de esta circunstancia y de la reanudación de las operaciones normales.

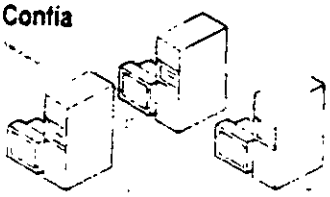

Finanzas
Finanzas Cuentas
SaraK
JuanP
TitoN
Conta
Ventas
C_DIR\ARCH1
Finanzas Cuentas L

Notas:



Finanzas

Confía

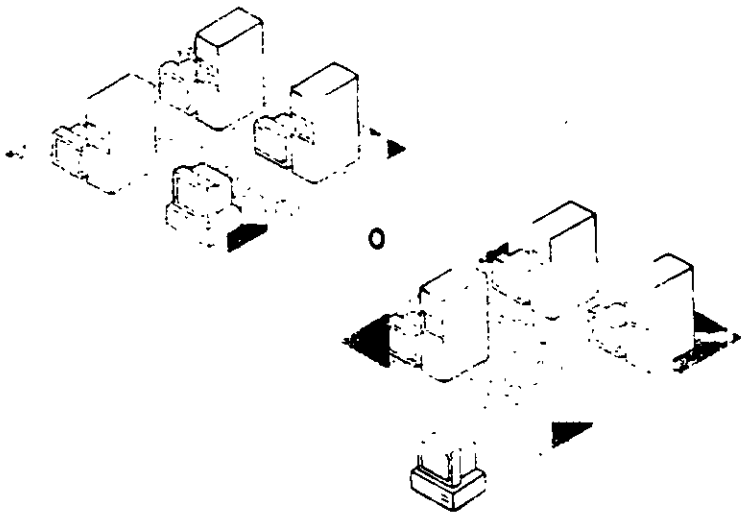


Ventas

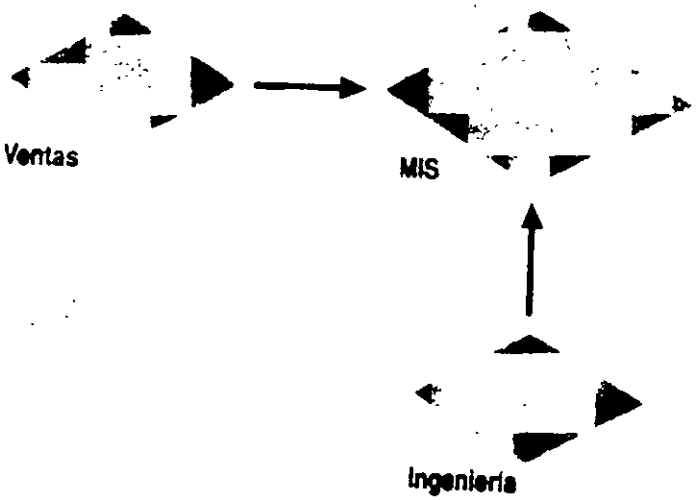
Organizadores.
JuanaB
Gerentes
Finanzas\Cuentas

C:\DIR\ARCH2;
Organizadores:LS

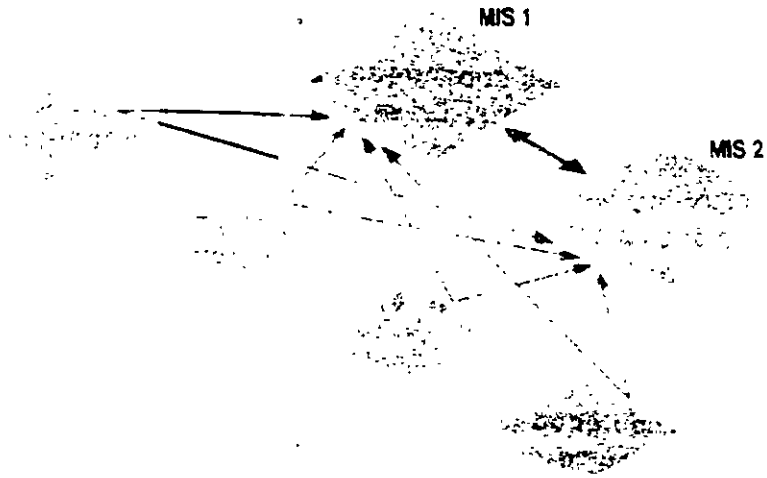
Notas:



Notas:



Notas:



Notas:

INSTALACIÓN Y MANEJO DE REDES (LAN)
CON WINDOWS NT Y/O
PRODUCTOS MICROSOFT

4.- INSTALACIÓN DE ELEMENTOS ESPECIALES

Mayo de 1996.

Administración de tolerancia a fallos y SAI

La *tolerancia a fallos* es la posibilidad de un sistema de continuar funcionando aunque falle parte del mismo. Normalmente, la expresión *tolerancia a fallos* se usa para describir subsistemas de disco, pero también puede aplicarse a otras partes del sistema o a su totalidad. Los sistemas totalmente tolerantes a fallos utilizan controladores de disco redundantes y fuentes de alimentación, así como también subsistemas de disco tolerantes a fallos. También se pueden utilizar sistemas de alimentación ininterrumpida (SAI) como protección frente a fallos de corriente locales.

Aunque los datos están siempre disponibles y actualizados en un sistema tolerante a fallos, aún es necesario realizar copias de seguridad en cinta para proteger la información de los discos frente a catástrofes como fuego, terremotos, tornados, inundaciones y errores de usuario. Los sistemas de discos tolerantes a fallos no son una alternativa a la estrategia de copias de seguridad con almacenamiento fuera de la instalación.

Concepto de RAID

Los sistemas de disco tolerantes a fallos están estandarizados, y clasificados en seis niveles denominados nivel 0 a nivel 5 de RAID (serie redundante de discos económicos). Cada nivel ofrece diversas combinaciones de características, seguridad y costo.

Los niveles de RAID están definidos de forma un tanto difusa, y los detalles acerca del rendimiento o uso del disco varían de una configuración a otra. Dependiendo de la implementación, las definiciones pueden superponerse o estar combinadas. Por ejemplo, en algunos hardware, se podrían utilizar los niveles 0 y 1 (división en bandas y conjunto de espejos) juntos para proporcionar lo último en redundancia y rendimiento, sin considerar el costo.

La diferencia fundamental entre RAID y tecnologías anteriores más costosas basadas en discos grandes (también llamadas de disco único, grande y caro, o SLED) es que RAID combina múltiples discos con niveles de seguridad individuales más bajos para reducir el costo total de almacenamiento. Este nivel inferior de seguridad se compensa con la redundancia.

Se debe tener en cuenta que no existe la tolerancia a fallos hasta que el fallo haya sido corregido. Pocas implementaciones de RAID pueden resistir simultáneamente dos fallos. Cuando se haya reemplazado el disco que ha fallado, los datos podrán regenerarse usando la información redundante (consulte el capítulo "Administrador de discos" en el *Manual de sistema de Windows NT* o en el *Manual de sistema de Windows NT Advanced Server* para obtener más información acerca de la reparación de conjuntos de espejos y conjuntos de bandas con paridad). Cuando se complete esta operación, todos los datos estarán actualizados y protegidos nuevamente frente a fallos de disco. Esto se producirá sin necesidad de utilizar cintas de copia de seguridad ni de realizar operaciones manuales de actualización para cubrir transacciones que tuvieran lugar después de la última copia de seguridad. La posibilidad de ofrecer una elevada disponibilidad de datos con costos razonables es la ventaja clave de las series de discos.

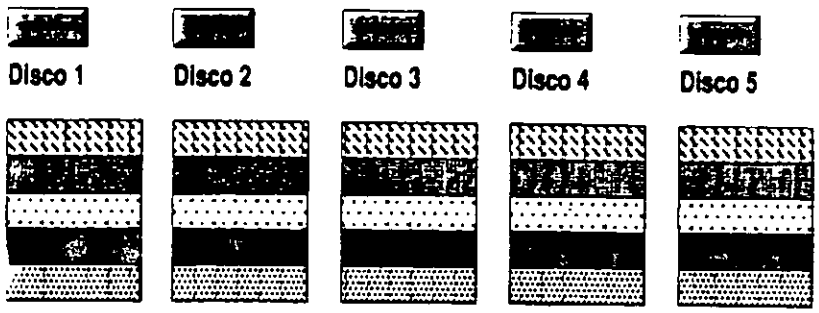
Nivel 0

Esta estrategia es conocida como *creación de bandas en discos* y utiliza un sistema de archivo de disco denominado *conjunto de bandas*. Los datos se dividen en bloques y se extienden en un orden fijo entre todos los discos de la serie. Esta estrategia es similar al nivel 5, que también tiene redundancia de datos.

La creación de bandas en disco de Windows NT escribe los datos en varias particiones, como ocurre con los conjuntos de volúmenes, pero en todos los discos, de manera que los datos se agregan a todas las particiones del conjunto en la misma proporción.

Este sistema ofrece el mejor rendimiento de todas las estrategias de la administración de discos de Windows NT Advanced Server, incluyendo los conjuntos de volúmenes. Sin embargo, al igual que éstos, no ofrece tolerancia a fallos. Si alguna partición de la banda falla, se perderán todos los datos.

Consulte el capítulo "Administrador de discos" en el *Manual de sistema de Windows NT* o en el *Manual de sistema de Windows NT Advanced Server* para obtener información acerca de la creación y eliminación de conjuntos de bandas. Consulte también la explicación acerca de seguridad de hardware en "Conceptos de seguridad", más adelante en este capítulo.



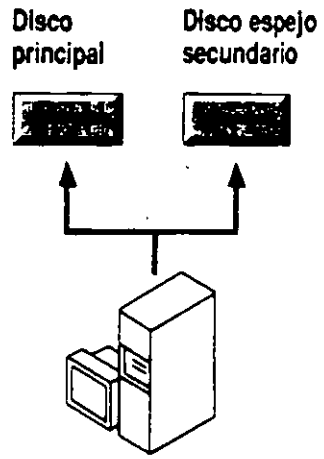
Nivel 0 de RAID

Nivel 1

Esta estrategia es conocida como *espejos de disco* y utiliza un sistema de archivo de disco denominado *conjunto de espejos*. Este método proporciona un disco espejo idéntico para un disco seleccionado; todos los datos que se escriban en el disco primario se escribirán en el disco gemelo o espejo. Esto da como resultado un uso del espacio en disco de sólo el 50 por ciento. Si un disco falla, el sistema utilizará los datos del otro disco (con excepción de los sectores de inicialización). Para obtener una explicación sobre cómo solucionar fallos de iniciación, consulte "Solución de fallos de iniciación", más adelante en este capítulo.

De las dos estrategias de tolerancia a fallos de Windows NT Advanced Server, el disco espejo posee mejor rendimiento global de lectura y escritura que los conjuntos de bandas con paridad. Otra ventaja de los conjuntos de espejos frente a los conjuntos de bandas con paridad es que no hay pérdida de rendimiento cuando un miembro del conjunto de espejos falla. El espejo de discos es más costoso en términos de precio por megabyte, ya que el uso del espacio en disco es menor. No obstante, su costo inicial es menor, ya que requiere sólo dos discos, mientras que los conjuntos de bandas con paridad necesitan tres o más. El conjunto de espejos de disco resulta adecuado para LAN establecidas entre iguales o bien para redes modestas basadas en servidor.

Consulte el capítulo "Administrador de discos" en el *Manual de sistema de Windows NT* o en el *Manual de sistema de Windows NT Advanced Server* para obtener información acerca de la creación y eliminación de conjuntos de espejos. Consulte también la explicación sobre seguridad de hardware en "Conceptos de seguridad", más adelante en este capítulo.



Nivel 1 de RAID

Nivel 2

Este método agrega redundancia mediante el uso de un código de corrección de errores. Emplea una estrategia de creación de bandas en disco que parte el archivo en bytes, dispersándolo entre diversos discos. El método de corrección de errores es bastante pesado y requiere varios discos para almacenar la información de corrección. Esta estrategia ofrece sólo una mejora marginal en el uso de disco con respecto al nivel 1. Constituye una mejora, desde el punto de vista histórico, sobre el espejo de discos, pero es pobre en comparación con la tecnología actual.

Nivel 3

Esta estrategia es similar al nivel 2 ya que emplea el mismo método de bandas. El método de corrección de errores requiere sólo un disco para datos de paridad. El uso del espacio en disco varía con el número de discos de datos y puede llegar a ser del 86 por ciento. Esta estrategia es mejor para aplicaciones que tienen acceso a un número reducido de archivos grandes.

Nivel 4

Esta estrategia emplea la división de datos en bandas de bloques o segmentos mucho mayores que los niveles 2 y 3. Aún mantiene todos los datos de corrección de errores en un solo disco, separados de los datos de usuario. Nuevamente, el uso del espacio varía con el número de discos de la serie.

Nivel 5

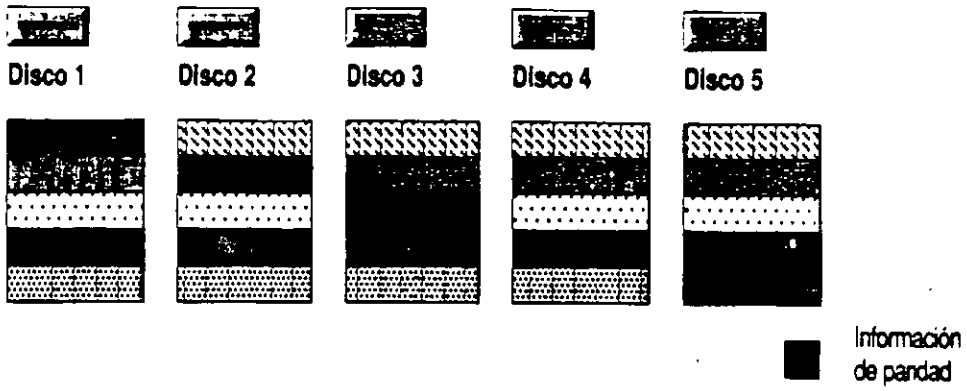
Esta estrategia es conocida como *creación de bandas con paridad*. Es la estrategia más extendida en los nuevos diseños. Es similar al nivel 4 en que distribuye los datos en bandas de grandes bloques en todos los discos de la serie. Se diferencia en que escribe la paridad en todos los discos. La redundancia de datos se proporciona por medio de la información de paridad. Los datos y la información acerca de la paridad están distribuidos en la serie de discos de forma que ambos estén siempre en discos distintos.

Los conjuntos de bandas con paridad tienen mejor rendimiento de lectura que el conjuntos de espejos. Sin embargo, cuando se pierde un miembro, por ejemplo cuando falla un disco, dicho rendimiento de lectura se degrada por la necesidad de recuperar los datos con la información de paridad.

No obstante, esta estrategia es más recomendable que el espejo de discos, en aplicaciones que requieran redundancia y estén principalmente orientadas a la lectura. El rendimiento de escritura se reduce a causa de los cálculos de paridad. Además, una operación de escritura requiere tres veces más memoria que una operación de lectura en condiciones normales y, cuando falla una partición, la lectura requiere al menos tres veces más memoria que la que se usaría normalmente, en ambos casos a consecuencia de los cálculos de paridad.

Nota El uso de conjuntos de bandas con paridad en Windows NT Advanced Server requiere más memoria del sistema que los conjuntos de espejos. El mínimo recomendable es de 12 MB de RAM, siendo preferible disponer de 16 MB o más.

Consulte el capítulo "Administrador de discos" en el *Manual de sistema de Windows NT* o en el *Manual de sistema de Windows NT Advanced Server* para obtener información acerca de la creación y eliminación de conjuntos de bandas con paridad. Consulte también la explicación acerca de seguridad de hardware en "Conceptos de seguridad", más adelante en este capítulo.



Configuración del nivel 5 de RAID

Planificación de un sistema tolerante a fallos

Como se mencionó anteriormente, se puede implementar la tolerancia a fallos de RAID tanto en el hardware como en el software. Windows NT Advanced Server ofrece tres de las estrategias de RAID en una solución de software. En una solución a nivel de hardware, la interfaz de controlador realiza la creación y regeneración de información redundante. En Windows NT Advanced Server, esta actividad se realiza a nivel de software.

Uso de soluciones de hardware

Las series de discos constituyen una solución muy utilizada para el almacenamiento de discos en servidores LAN de alto rendimiento. Constan de múltiples mecanismos de disco coordinados por un controlador. Los archivos de datos individuales se escriben normalmente en más de un disco de forma que, dependiendo del nivel de RAID utilizado, se puedan mejorar el rendimiento y/o la seguridad.

Una implementación hardware de un nivel de RAID puede ofrecer ventajas en cuanto a rendimiento sobre el uso de las estrategias de RAID de Windows NT Advanced Server. Se puede alcanzar al nivel 5 de RAID a través de soluciones de hardware, tales como adaptadores de series de discos, que no utilizan ningún recurso de software, como pueden ser las soluciones de tolerancia a fallos de Windows NT Advanced Server. Esto mejora significativamente la capacidad de tratamiento de datos. La clave es el uso de más discos para una capacidad determinada que en una solución de almacenamiento convencional. Si utiliza controladores múltiples en un enfoque inteligente, las operaciones de lectura y escritura pueden mejorarse significativamente respecto de SLED.

Las implementaciones hardware de las estrategias de RAID pueden ofrecer muy buenos resultados, dependiendo de la configuración. Se puede incluso reemplazar una unidad en la que se ha producido un fallo sin necesidad de apagar el sistema. Las desventajas de dichas soluciones de hardware son su elevado costo y la posibilidad de quedar bloqueado en la solución de un único fabricante.

Uso de la solución de software de Windows NT

El sistema operativo de Windows NT Advanced Server implementa varias de las estrategias de RAID con el hardware de disco o la interfaz de cualquier fabricante. Dichas estrategias incluyen:

- Conjuntos de bandas (nivel 0 de RAID).
- Conjuntos de espejos (nivel 1 de RAID).
- Conjuntos de bandas con paridad (nivel 5 de RAID).

En Windows NT Advanced Server, los conjuntos de bandas ofrecen los mejores rendimientos pero no tolerancia a fallos (es decir, redundancia de datos).

Cuando se compara con los conjuntos de bandas con paridad, la implementación de un conjunto de espejos tiene un menor costo inicial, requiere menos memoria del sistema, ofrece mejores rendimientos globales y no muestra degradación de los rendimientos durante un fallo. No obstante, su costo por megabyte es más elevado que en el caso de conjuntos de bandas con paridad.

La implementación de un conjunto de bandas con paridad tiene mejores operaciones de lectura y un costo inferior por megabyte, pero requiere más memoria del sistema y pierde sus ventajas en cuanto a rendimiento cuando se pierde uno de sus miembros.

Conceptos de seguridad

Observe que la adición de discos como un conjunto de volúmenes o bandas *reduce* la seguridad del subsistema de disco, ya que no hay redundancia de información. Si alguno de los discos del conjunto falla, todos los datos del conjunto de volúmenes o bandas se perderán. La seguridad del hardware es la misma para conjuntos de espejos y bandas con paridad, pero estas estrategias ofrecen una segura redundancia de la información.

La posibilidad de un fallo de un disco se describe típicamente por medio de una unidad estadística denominada *tiempo medio entre fallos* (MTBF), medida en horas. La probabilidad de un fallo de hardware en un subsistema de disco se calcula de la forma siguiente:

$$MTBF_{conjunto} = MTBF_{disco}/N$$

donde $MTBF_{conjunto}$ es el MTBF del conjunto, $MTBF_{disco}$ es el MTBF de cualquiera de los discos individuales de la serie (asumiendo que son idénticos) y N es el número de discos del conjunto.

Por ejemplo, un conjunto de cuatro discos tiene un tiempo entre fallos igual a la cuarta parte del tiempo entre fallos de un disco aislado o, en otras palabras, es cuatro veces más probable que falle en un período de tiempo determinado. Esto se considera una debilidad que puede ser significativa en sistemas que dan una alta prioridad a la disponibilidad de los datos actuales. Esto también incrementa la importancia de una buena estrategia de copias de seguridad.

Uso de la paridad en Windows NT

El método de redundancia de datos usado en Windows NT Advanced Server para la división en bandas con paridad es una función Booleana denominada *OR exclusivo* o XOR. El concepto importante que hay que recordar acerca de la paridad es que el proceso de regeneración utiliza la información de paridad y de los datos en los discos en buen estado para volver a crear los datos del disco que ha fallado. La tolerancia a fallos por medio de conjuntos de bandas con paridad de Windows NT Advanced Server mantiene un XOR sobre la totalidad de los datos. Esto permite la reconstrucción de los datos perdidos (de un disco o sector que haya fallado) a partir del resto de los discos del conjunto de bandas con paridad.

Sustitución de sectores de disco defectuosos

El sistema de archivos verifica todos los sectores cuando formatea un volumen. Se apartan del servicio todos los sectores defectuosos. Otros servicios de tolerancia a fallos de Windows NT agregan posibilidad de recuperación de sectores al sistema.

Cuando se produce un fallo de E/S en un sistema tolerante a fallos con copias redundantes de los datos, el controlador de tolerancia a fallos de Windows NT intenta sustituir los sectores defectuosos. Esto incluye realizar un control de dispositivos, indicando al controlador de disco que no utilice el sector. Los dispositivos de Interfaz estándar de computadoras pequeñas (SCSI) pueden hacerlo, pero los dispositivos AT, es decir, Electrónica integrada de dispositivos (IDE) e Interfaz mejorada de dispositivos pequeños (ESDI), no pueden. Cuando no se puede sustituir el sector, la información correcta obtenida de la copia redundante se devuelve al sistema de archivos con un mensaje de estado que indica la existencia de un sector de E/S defectuoso. El sistema de archivos de Windows NT (NTFS) reacciona ante dicho mensaje intentando localizar el fallo y apartar los sectores defectuosos del servicio, quitándolos del mapa de sectores del sistema de archivos. También se notifica al administrador en el Visor de sucesos de la pérdida potencial de datos si también falla la partición que contiene la copia redundante.

Solución de fallos de iniciación

Si la partición de inicialización de un disco falla, el sistema no se iniciará. El proceso utilizado en la recuperación de un fallo de iniciación depende de la configuración del disco y del tipo de microprocesador del sistema de la computadora. Si la partición de inicialización del disco no forma parte de un conjunto de espejos, se deberá restaurar la copia de seguridad del sistema en el disco de reemplazo.

En una partición de inicialización configurada como parte de un conjunto de espejos, el proceso de recuperación depende de si la computadora (ordenador) está basada en un procesador x86 o RISC. Ambos utilizan un disquete para la protección de inicialización y de nombres ARC (Computación avanzada de RISC) para describir el proceso de inicialización.

Funcionamiento del servicio de SAI

La opción SAI del Panel de Control de Windows NT permite la comunicación entre el servicio de SAI y el dispositivo SAI a través de un puerto serie con las siguientes señales:

Señal de	Patilla	Activado por
Fallo de alimentación eléctrica	CTS (permiso para enviar)	El hardware del SAI
Pila con poca carga	DCD (Detector de portadora de datos)	El hardware del SAI
Apagado de SAI	DTR (Terminal de datos preparada)	El servicio de SAI de Windows NT

La señal de cada una de estas patillas puede ser positiva o negativa, dependiendo de la implementación del dispositivo SAI. Utilice el cuadro de diálogo **SAI** para especificar la polaridad utilizada por el hardware del SAI.

Para funcionar con dispositivos SAI del tipo cierre de contactos, el servicio de SAI siempre configura lo siguiente:

- Establecer la patilla 6, TXD (Transmisión de datos), permanentemente en estado bajo.
- Establecer la patilla RTS (Petición para emitir) permanentemente en estado alto.

Cuando se inicia el servicio de SAI, éste verifica la configuración del cuadro de diálogo **SAI** asumiendo que el sistema no se está iniciando durante un corte de alimentación eléctrica y asegurándose de que la polaridad de la señal en las patillas CTS y DCD es opuesta a la especificada como condición de fallo en dicho cuadro de diálogo. Por ejemplo, si el cuadro de diálogo **SAI** especifica que el dispositivo SAI transmite un aviso de corte de alimentación eléctrica (patilla CTS) con señal positiva, el servicio de SAI verificará que dicha patilla no presente una señal positiva, cosa que no debería suceder a menos que el sistema se iniciara durante un corte de alimentación eléctrica.

Esto tiene algunas implicaciones importantes. En un SAI directo, el dispositivo puede apagarse inmediatamente si la configuración es incorrecta. En el caso de SAI directo, una configuración incorrecta normalmente apaga el dispositivo SAI cuando se produce un corte en la alimentación eléctrica, anulando el propósito del SAI. Por esta razón es importante configurar y probar el dispositivo SAI para asegurarse de que funciona correctamente.

Cuando se inicia el servicio de SAI, éste espera hasta que el SAI envíe una señal a la patilla CTS. Si se ha indicado en el cuadro de diálogo **SAI** que el dispositivo SAI no transmite el aviso de pila con poca carga, el servicio de SAI usará el parámetro especificado en el cuadro "Características del SAI" del cuadro de diálogo **SAI** para estimar el nivel de carga de la pila en minutos. Cada vez que se inicie el servicio de SAI, se restablecerá el nivel de carga de la pila en 0 minuto. Conforme pase el tiempo, se usará el parámetro "Tiempo de recarga de la pila" para estimar la duración de la pila hasta un tiempo máximo especificado por el parámetro "Duración estimada de la pila". El servicio de SAI requiere al menos 2 minutos para realizar correctamente un apagado correcto del sistema. Por lo tanto, si en algún momento la duración de la pila no es superior a 2 minutos, se realizará un apagado inmediato. Como es importante que los parámetros del cuadro "Características del SAI" se establezcan de forma precisa, lo mejor es usar las estimaciones más pesimistas.

Cuando ocurre un corte en la alimentación eléctrica, el servicio de SAI usa los parámetros del cuadro "Servicio de SAI" del cuadro de diálogo **SAI** para decidir el modo de respuesta. En caso de ruidos de alimentación (es decir, corriente que fluctúa de forma regular), se debe establecer el primer parámetro en unos pocos segundos. Esto minimiza la difusión de mensajes. El dispositivo SAI envía continuamente mensajes con un intervalo especificado por el segundo parámetro del cuadro "Servicio de SAI". Este debe establecerse en un valor muy bajo si desea que los usuarios estén prevenidos ante un corte en la alimentación eléctrica o, por el contrario, en un valor alto si no es importante advertirlos de dicho corte. Cuando la pila del SAI tenga poca carga, el servicio inicia un apagado y luego desconecta el dispositivo SAI (si tiene esta característica).

Uso de un SAI con Windows NT

Debería usar los siguientes servicios de Windows NT en combinación con el dispositivo SAI seleccionado para su computadora (ordenador):

- Servicio de SAI
- Servicio de Alerta
- Servicio de Mensajería
- Servicio de Registro de sucesos

A continuación se explican algunos puntos básicos que se deben tener en cuenta para asegurar que el SAI esté correctamente instalado y mantener su computadora protegida de los riesgos de un corte en la alimentación eléctrica.

Un dispositivo SAI proporciona corriente a su computadora, y periféricos (por ejemplo, monitor e impresora) cuando se interrumpe o falla completamente la alimentación eléctrica. Algunos dispositivos SAI pueden suministrar corriente eléctrica sólo durante unos pocos minutos, mientras que otros pueden hacerlo durante muchas horas. En cualquier caso, debe establecer correctamente una interfaz entre el dispositivo SAI y Windows NT, de forma que el SAI pueda detectar las fluctuaciones de corriente y realizar las acciones adecuadas. Por ejemplo, si un corte fuera prolongado, el SAI no podría suministrar corriente durante todo el intervalo del fallo. En este caso, Windows NT advertiría a los usuarios de dicho corte. Cuando el SAI llegue a un estado crítico, se realizará un apagado del sistema operativo y el dispositivo SAI se desconectará. Por lo tanto, debería asegurar que su dispositivo SAI garantiza al menos 2 minutos para permitir al sistema operativo realizar un apagado correcto.

Seleccione un dispositivo SAI que funcione con Windows NT. Normalmente, esto significa encargar el cable serie correcto al fabricante del SAI. Dicho cable estará diseñado siguiendo las especificaciones de la interfaz de SAI con Windows NT. Si está instalando Windows NT en su computadora (ordenador) y ya posee un SAI, verifique con el fabricante que el cable existente funcione con Windows NT. Pueden obtenerse resultados inesperados si se utiliza un cable incorrecto.

Los fabricantes de SAI pueden disponer de su propio software que puede adquirirse separadamente y de este modo aprovechar las ventajas especiales de sus dispositivos SAI. En este caso, no debería usar el servicio de SAI que se suministra con Windows NT. Siga las instrucciones que acompañan al software del fabricante.

El servicio de SAI se configura por medio del cuadro de diálogo **SAI**. Debería configurarlo basándose en las características admitidas por el dispositivo SAI que esté usando. Las tres características admitidas por Windows NT son:

- Detección de corte de alimentación.
- Detección de pila con poca carga.
- Posibilidad de apagado del SAI.

Para determinar la configuración correcta, lea cuidadosamente el manual de usuario de su dispositivo SAI o póngase en contacto con el fabricante. Dependiendo de las características admitidas por el SAI, puede ser necesario introducir parámetros adicionales en el cuadro "Características del SAI" del cuadro de diálogo **SAI**.

El servicio de SAI se puede controlar de diversas maneras. Una de ellas es configurar los parámetros del cuadro de diálogo **SAI** y seleccionar el botón "Aceptar". Aparecerá un mensaje preguntando si se desea iniciar el servicio de SAI. Otra manera de iniciar el servicio es utilizar la opción "Servicio" del Panel de control.

Los servicios de Alerta y Mensajería deben iniciarse manualmente usando la opción "Servicios" del Panel de control. El servicio de Alerta envía mensajes de alerta a los usuarios seleccionados, y el de Mensajería envía mensajes a su computadora local con Windows NT y a otros usuarios de la red. Todas las fluctuaciones y cortes de alimentación eléctrica se anotan en el registro de sucesos, junto con los inicios del servicio de SAI (o fallos de inicio) e inicios de apagado del servidor.

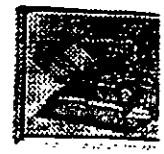
Para asegurarse de que la computadora esté protegida frente a cortes de alimentación, apague la fuente de alimentación principal del dispositivo SAI. Su computadora y periféricos conectados con el dispositivo SAI deberán permanecer en funcionamiento, y deberán mostrar mensajes y registrar sucesos. Espere a que la batería alcance un nivel bajo para verificar que ocurrirá un apagado correcto. Restaure la alimentación principal del dispositivo SAI y compruebe el registro de sucesos, para asegurarse de que se registraron todas las acciones y de que no hubo errores.

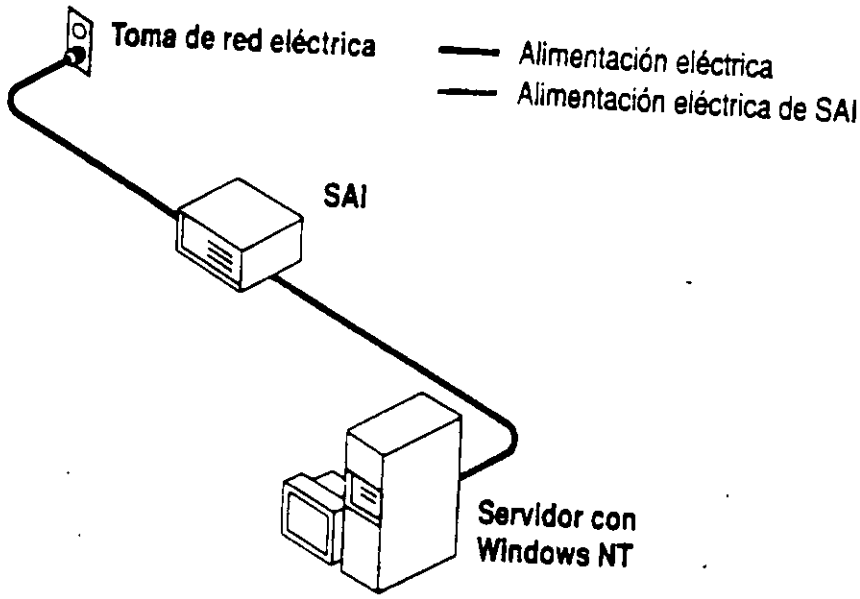
Ejecución de un archivo de comandos durante el apagado de SAI

El servicio de SAI de Windows NT permite la ejecución de un archivo de comandos definido por el administrador. Sólo debería especificar un archivo de comandos si su sistema requiriese acciones especiales previas al apagado del sistema. Por ejemplo, puede tener en ejecución una aplicación personalizada conectada a otra computadora (ordenador). En este caso, podría usar un archivo de comandos para finalizar la sesión y cerrar la conexión automáticamente antes del apagado del sistema.

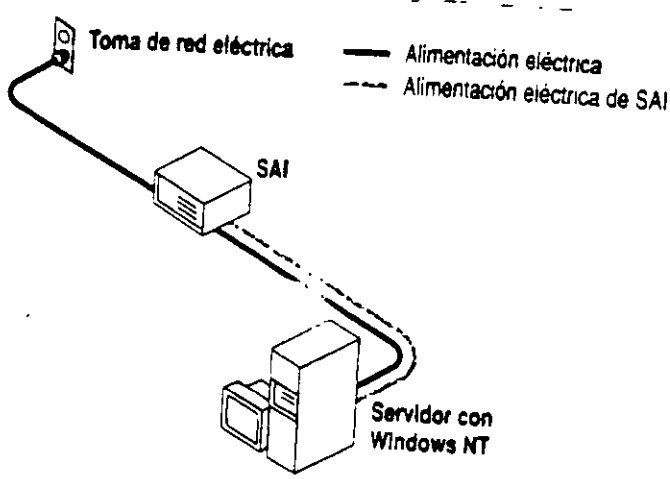
El archivo de comandos debe residir en su directorio [*raíz_del_sistema*]\SYSTEM32 y tener una de las siguientes extensiones: .EXE, .COM, .BAT o .CMD. Después de crear el archivo y situarlo en el directorio apropiado, utilice el cuadro de diálogo **SAI** para activar su uso durante el apagado del SAI. Seleccione la opción "Ejecutar archivo de comandos", escriba el nombre del archivo y seleccione el botón "Aceptar".

Nota El archivo de comandos debe finalizar su ejecución en 30 segundos. Un tiempo de ejecución mayor amenaza la capacidad de Windows NT para completar un apagado correcto del sistema. Debería comprobar el funcionamiento del archivo de comandos en el caso más desfavorable.




Toma de red eléctrica
Alimentación eléctrica
Alimentación eléctrica de SAI
SAI
Servidor con
Windows NT

Notas:


Toma de red eléctrica
Alimentación eléctrica
Alimentación eléctrica de SAI
SAI
Servidor con
Windows NT

Notas:

INSTALACIÓN Y MANEJO DE REDES (LAN) CON WINDOWS NT Y/O PRODUCTOS MICROSOFT

5.- EL ADMINISTRADOR Y SUS FUNCIONES

Mayo de 1996.

Administración de entornos de usuario

En una red de Windows NT Advanced Server existen diversos procedimientos para definir y optimizar los entornos de las estaciones de trabajo de los usuarios. Es posible definir las conexiones de red, las aplicaciones disponibles, los grupos de programas de Windows y el aspecto del escritorio de Windows. Incluso, si lo desea, puede impedir que los usuarios de las estaciones de trabajo con Windows NT cambien la configuración del escritorio que se haya creado.

El método más potente para administrar los entornos de los usuarios es la asignación de *perfiles de usuario* a los usuarios de las estaciones de trabajo con Windows NT. Un perfil es un archivo que actúa como una instantánea del entorno del escritorio del usuario, definiendo los grupos del Administrador de programas y los elementos de programa contenidos en dichos grupos, las conexiones de impresora, el tamaño y la posición de las ventanas, y los colores de la pantalla. Los perfiles permiten también limitar a los usuarios que modifiquen estas características en sus propias estaciones de trabajo.

Otra forma de mejorar los entornos de los usuarios consiste en asignarles *archivos de comandos de inicio de sesión*. Si un usuario tiene uno de estos archivos, éste se ejecutará cada vez que inicie una sesión en cualquier tipo de estación de trabajo de la red. Este archivo de comandos de inicio de sesión puede ser un archivo por lotes que incluye comandos del sistema operativo (por ejemplo, los comandos necesarios para establecer las conexiones de red o iniciar aplicaciones) o un programa ejecutable.

También se puede optar por proporcionar a cada usuario un *directorio base* en un servidor o estación de trabajo. El directorio base de un usuario proporcionará a dicho usuario un espacio de almacenamiento privado. Cada usuario tendrá control sobre el contenido y el acceso a su directorio base.

También es posible establecer las *variables de entorno* de cada estación de trabajo. Las variables de entorno especifican la ruta de búsqueda de la estación de trabajo, el directorio donde se almacenan los archivos temporales, además de otra información similar.

Funcionamiento de los perfiles de usuario

Los perfiles de usuario contienen las características del entorno Windows NT de cada usuario. La siguiente tabla muestra exactamente lo que se ha guardado en un perfil.

Los perfiles de usuario solamente resultan útiles para aquellos usuarios que trabajen en estaciones de trabajo con Windows NT. No tienen ningún efecto sobre los usuarios que utilicen estaciones de trabajo con MS-DOS.

Las estaciones de trabajo con Windows NT incorporan algunos aspectos de los perfiles de usuario. En una red que utilice Windows NT Advanced Server, existen muchas maneras de aumentar la utilidad de los perfiles. Sin embargo, antes de aprender a hacerlo, conviene que entienda perfectamente el modo en que los perfiles de usuario funcionan en las estaciones de trabajo con Windows NT.

Características que se guardan en un perfil de usuario

Origen	Parámetros guardados
Administrador de programas	Todas las opciones del Administrador de programas definibles por el usuario, como los grupos de programas personales y sus propiedades, los elementos de programa y sus propiedades, y todas las opciones que se guardan al elegir los comandos **Guardar configuración al salir** o **Guardar configuración ahora**.
Administrador de archivos	Todas las opciones del Administrador de archivos definibles por el usuario, entre las cuales se incluyen las conexiones de red y todas las características que se guardan cuando está seleccionado el comando **Guardar configuración al salir**.
Interfaz de comandos	Todas las opciones de la interfaz de comandos definibles por el usuario, como las fuentes, los colores, las características de tamaño del búfer de pantalla y la posición de la ventana.
Administrador de impresión	Las conexiones de impresoras de red y todas las opciones que se guardan cuando está seleccionado el comando **Guardar configuración al salir**.
Opciones del Panel de control	Todas las opciones de Color, Mouse, Escritorio, Cursor, Teclado, Internacional y Sonido. Para la opción "Sistema", solamente se guardarán los datos del cuadro *"Variables de entorno de usuario"*. Las demás opciones del Panel de control no contienen ninguna característica específica del usuario.

Características que se guardan en un perfil de usuario

Origen	Parámetros guardados
Accesorios	Todas las opciones de cada aplicación específicas del usuario, que afecten a su entorno Windows NT. Entre las aplicaciones de Accesorios se encuentran Calculadora, Fichero, Reloj, Portafolio, Paintbrush y Terminal.
Aplicaciones para Windows NT de otros fabricantes	Cualquier aplicación que haya sido desarrollada específicamente para Windows NT podrá diseñarse de tal modo que mantenga las características de la aplicación para cada usuario. Si existe esta información, se guardará en el perfil de usuario.
Marca-texto de la Ayuda en pantalla	Cualquier marca-texto que se haya introducido en el sistema de Ayuda de Windows NT.

Perfiles locales en estaciones de trabajo con Windows NT

Los perfiles locales son creados siempre por Windows NT de forma automática, sin que el administrador deba encargarse expresamente de ello. Cada vez que un usuario (excepto aquellos usuarios que no puedan mantener perfiles locales) inicie una sesión y posteriormente cierre esa sesión en una estación de trabajo con Windows NT, el sistema guardará en un perfil local las opciones que haya seleccionado el usuario.

Nota Los miembros de los grupos Administradores, Usuarios avanzados, Usuarios y Operadores de copia de seguridad tienen la posibilidad de mantener perfiles locales en las estaciones de trabajo con Windows NT. Los miembros del grupo local Invitados no disponen de este derecho (a menos que sean también miembros de alguno de los grupos locales que sí puedan hacerlo).

Entre estas características se incluyen las conexiones de red, los grupos y elementos de programa, el tamaño y la posición de la ventana, y el aspecto de la pantalla. Cuando el usuario vuelva a iniciar una sesión en una estación de trabajo, ésta reconocerá al usuario y cargará el perfil que se creó la última vez que el usuario cerró una sesión en esa estación de trabajo.

Los perfiles garantizan que todo usuario pueda disponer de sus preferencias cada vez que inicie una sesión. En las estaciones de trabajo que son utilizadas por distintas personas, los perfiles permiten a cada usuario configurar un entorno personalizado. El entorno de un usuario puede ser distinto del que utilicen los demás usuarios de esa estación de trabajo, pero se mantendrá cada uno de los entornos y se cargará el apropiado cuando un usuario inicie una sesión.

Los perfiles locales dependen de la computadora (ordenador): las opciones que seleccione un usuario en una estación de trabajo no estarán a su disposición cuando dicho usuario inicie una sesión en otra estación de trabajo diferente.

Ventajas de los perfiles basados en servidor

En las redes con dominios y Windows NT Advanced Server, es posible crear perfiles para aquellos usuarios que dispongan de cuentas de dominio y almacenar dichos perfiles en los servidores. Esta posibilidad aumenta la utilidad de los perfiles, en tres aspectos:

- Cada usuario puede tener un perfil individual, con una configuración que se cargará cada vez que inicie una sesión en cualquier estación de trabajo con Windows NT.
- Es posible utilizar el perfil para limitar la posibilidad de acceso del usuario a su estación de trabajo, impidiéndole que modifique determinados aspectos de su configuración.
- Si muchos usuarios utilizan un mismo perfil, es posible otorgar a todos ellos el acceso a una nueva aplicación o servidor, con sólo editar ese perfil.

Las dos primeras ventajas se consiguen gracias a ambos tipos de perfiles de servidor: *perfiles personales* y *perfiles obligatorios*. La tercera ventaja sólo se consigue con los perfiles obligatorios. En las secciones siguientes se explican con mayor detalle las diferencias entre los perfiles personales y obligatorios:

Diferencias entre los perfiles personales y obligatorios

Tanto los perfiles personales como los obligatorios se almacenan en servidores. En ambos casos es posible asignar un perfil a un usuario especificando en su cuenta de usuario la ubicación y el nombre de archivo del perfil. Cada usuario sólo puede tener asignado un perfil.

Las extensiones del nombre de archivo de los perfiles personales deben ser .USR. Los perfiles obligatorios deben tener la extensión .MAN.

Los usuarios de perfiles personales pueden modificar de manera permanente sus perfiles. Aunque el usuario no será consciente de que está modificando su perfil, cada vez que cierre una sesión en una estación de trabajo, se guardarán los cambios que haya introducido en las características específicas del usuario. Cuando posteriormente dicho usuario vuelva a iniciar una sesión, se restablecerá el entorno que existiera la última vez que cerró una sesión.

Los usuarios de perfiles obligatorios no pueden introducir modificaciones de manera permanente en sus perfiles. Aunque un usuario que disponga de un perfil obligatorio puede modificar las características específicas del usuario a lo largo de una sesión, dichos cambios no se transferirán al perfil de usuario cuando éste cierre la sesión. Cuando el usuario vuelva a iniciar una sesión, se restablecerán las características originales del perfil, que no incluirán ninguno de los cambios realizados.

Utilidad de los perfiles personales

La principal aplicación de los perfiles personales consiste en permitir que las preferencias y opciones de cada usuario lo acompañen de una estación de trabajo a otra. Esto resulta claramente útil en aquellas redes en las cuales los usuarios utilicen a menudo distintas estaciones de trabajo. Sin embargo, también puede ser útil en otras situaciones. Por ejemplo, cuando la computadora de un usuario sea sustituida por otra más potente, la existencia de un perfil personal garantizará que las preferencias del usuario estén accesibles inmediatamente en la nueva computadora (ordenador).

Si lo desea, también puede introducir opciones en un perfil que limiten la posibilidad del usuario para modificar su propio entorno de trabajo. Si desea ver la lista de las restricciones que puede especificar, consulte la sección "Uso de perfiles para restringir las capacidades del usuario", que aparece más adelante *en este mismo capítulo.*

Con los perfiles personales, cada usuario puede tener su propio perfil. Es recomendable que el nombre de archivo de cada uno de los perfiles personales coincida exactamente con el nombre de usuario de quien vaya a utilizarlo; por ejemplo, el usuario JuanA podría tener el perfil JUANA.USR. De este modo, si se crea una nueva cuenta de usuario copiando la cuenta de JuanA, el nuevo usuario tendrá como nombre de perfil su propio nombre de usuario. Por ejemplo, si crea una nueva cuenta MaríaB copiando la cuenta JuanA, si el perfil de JuanA es JUANA.USR, el perfil de MaríaB será MARIAB.USR.

Utilidad de los perfiles obligatorios de usuario

Los perfiles obligatorios de usuario permiten a un usuario tener un mismo entorno de escritorio en cualquier estación de trabajo, del mismo modo que los perfiles personales.

Si se utilizan perfiles obligatorios, es posible también impedir que los usuarios puedan modificar sus propios perfiles. Ningún cambio en el entorno que realice un usuario a lo largo de una sesión (en caso de que el perfil de usuario le permita realizar cambios) se guardará en el perfil obligatorio del usuario. Cuando el usuario cierre la sesión y vuelva a iniciarla, se restablecerá el entorno original especificado en el perfil.

Por este motivo, los perfiles obligatorios resultan de mayor utilidad cuando se desea limitar las posibilidades del usuario en sus propias estaciones de trabajo. En la sección siguiente de este capítulo encontrará una lista de las restricciones que puede aplicar.

Puesto que a menudo un mismo perfil obligatorio se asigna a muchos usuarios, otra de sus ventajas es la posibilidad de actualizar fácilmente los entornos de numerosos usuarios a la vez. Por ejemplo, si necesita incorporar un nuevo elemento de programa para varios usuarios, bastará con que lo agregue a su perfil obligatorio.

Si se utilizan perfiles personales en lugar de obligatorios, no resultará práctico otorgar a los usuarios el acceso a nuevos servidores editando sus perfiles, ya que habría que cambiar individualmente el perfil de cada uno de los usuarios. Si en su red se utilizan perfiles personales y desea poder actualizar las conexiones de un usuario, deberá considerar el empleo de archivos de comandos de inicio de sesión. Si desea obtener más información al respecto, consulte la sección "Funcionamiento de los archivos de comandos de inicio de sesión" que aparece más adelante en este mismo capítulo.

Uso de perfiles para restringir las capacidades de los usuarios

Tanto en los perfiles personales como en los obligatorios, es posible impedir que un usuario pueda realizar una o varias de las siguientes operaciones:

- Crear elementos de programa
- Crear grupos de programas
- Cambiar el contenido de los grupos de programas
- Cambiar las propiedades de un elemento de programa (por ejemplo, la aplicación que se iniciará cuando se elija el elemento de programa)
- Ejecutar programas desde el menú **Archivo** del Administrador de programas
- Establecer conexiones con impresoras de red (distintas de las impresoras con las cuales establezca conexiones el propio perfil)

La posibilidad de aplicar alguna de estas restricciones o todas ellas sobre determinados usuarios resulta de suma utilidad en un entorno protegido, como puede ser un banco. En este tipo de entornos, probablemente será necesario crear un único perfil obligatorio para cada tipo de trabajo y posteriormente asignar dicho perfil a todos los usuarios cuyo trabajo se ajuste a esa clasificación, por ejemplo, un perfil CAJEROS.MAN para todos los cajeros del banco.

Concepto de perfil predeterminado

Toda estación de trabajo con Windows NT contiene un archivo predeterminado de perfil de usuario, que se cargará cada vez que un usuario inicie una sesión en alguno de los siguientes casos:

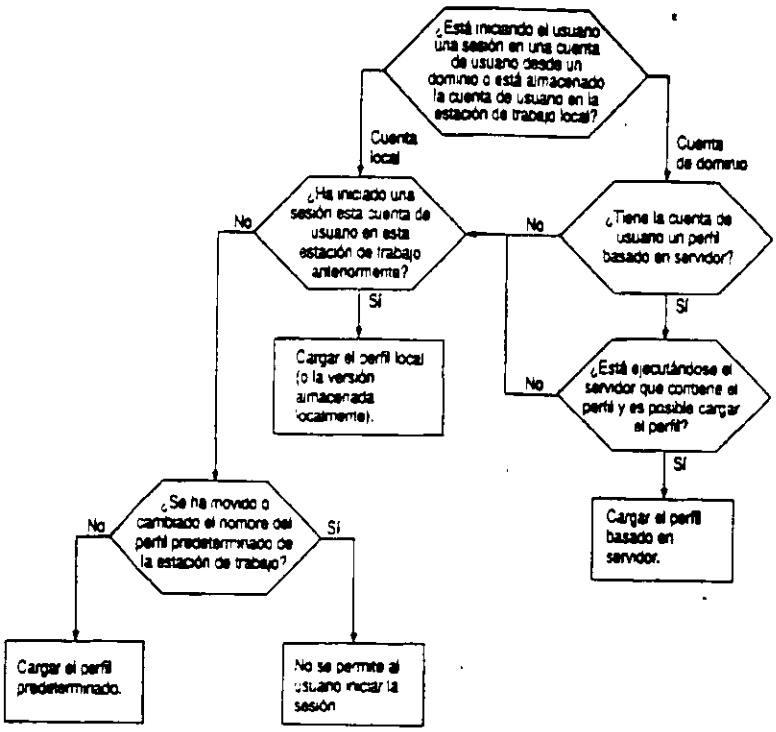
- Cuando la cuenta del usuario no tenga asignado ningún perfil y el usuario no haya iniciado nunca una sesión en esta computadora (ordenador) con Windows NT
- Cuando el perfil asignado a la cuenta del usuario no esté accesible durante el inicio de sesión (por ejemplo, porque esté apagado el servidor donde está almacenado el perfil) y el usuario no haya iniciado nunca una sesión en esta computadora
- Cuando un usuario inicie una sesión con la cuenta Invitado

Cuando una cuenta de usuario no tenga asignado ningún perfil de usuario, la primera vez que dicho usuario inicie una sesión en una determinada estación de trabajo con Windows NT, se utilizará el perfil predeterminado de esa estación de trabajo. Posteriormente (si el usuario está autorizado a tener un perfil local), al cerrar la sesión se guardarán las características específicas del usuario, que se convertirán en el perfil local de dicho usuario para esa estación de trabajo. Cada vez que el usuario vuelva a iniciar una sesión en esa estación de trabajo, Windows NT cargará la copia local que se guardó la última vez que inició una sesión, en lugar del perfil predeterminado de la estación de trabajo.

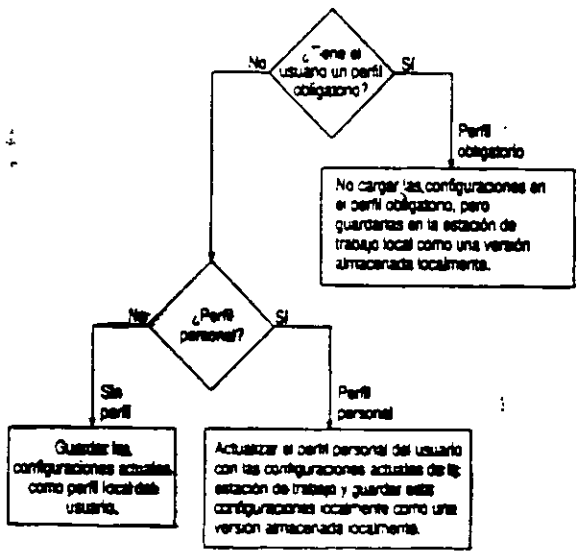
Cuando se instala Windows NT, el perfil predeterminado no establece ninguna restricción severa para los usuarios que inicien una sesión con él. Por consiguiente, en las redes protegidas será conveniente modificar los perfiles predeterminados de la computadora (ordenador) para que no permitan un nivel de acceso mayor que el del perfil más restrictivo existente.

Carga y descarga de perfiles

En los siguientes diagramas se ilustra el proceso que tiene lugar cuando un usuario inicia y cierra una sesión en una estación de trabajo con Windows NT. Si desea obtener más información sobre las versiones guardadas localmente de los perfiles de usuario basados en servidor que se mencionan en el diagrama, consulte la sección siguiente.



Carga de perfiles.



Almacenamiento de perfiles.

Copia local de perfiles

La mayoría de los usuarios están autorizados a mantener un perfil local en una estación de trabajo con Windows NT.

Cada vez que un usuario cierre una sesión en una estación de trabajo con Windows NT, se guardarán en un perfil local las características propias del usuario que existiesen en el momento en que dicho usuario cerró la sesión. Si el usuario no dispone de ningún perfil basado en servidor, éste será el único perfil que existirá para ese usuario. Si el usuario dispone además de un perfil personal basado en servidor, lo que se guardará en la estación de trabajo será una copia local del perfil del usuario. Esta versión local se utilizará cada vez que inicie una se[illegible]lgún usuario que disponga de un perfil basado en servidor, pero no sea p[illegible] acceder al servidor que contiene ese perfil.

Si u[illegible]rio posee un perfil personal, en el momento en que dicho usuario cierre una sesión, las características específicas se guardarán tanto en el perfil personal del usuario como en la copia local. El perfil local es idéntico al perfil personal actualizado.

Si un usuario posee un perfil obligatorio, los cambios que realice durante el transcurso de una sesión no se transferirán al perfil obligatorio cuando cierre la sesión, es decir, que nunca podrá modificar el perfil obligatorio. Sin embargo, si el perfil obligatorio le permite realizar cambios durante una sesión, cualquier modificación que efectúe se guardará en la versión local del perfil obligatorio. De este modo, la próxima vez que el usuario inicie una sesión en esta estación de trabajo, si no le es posible acceder a su perfil obligatorio, se cargará el perfil local y dispondrá de los cambios que haya realizado durante el transcurso de su última sesión.

Si un usuario inicia una sesión y no están disponibles ni el perfil basado en servidor ni la copia local de dicho perfil, se utilizará el perfil predeterminado de esa estación de trabajo. Si el usuario tiene un perfil obligatorio, no podrá iniciar una sesión.

Grupos de programas personales y comunes en los perfiles

Con Windows NT, todo grupo de programa pertenece a uno de los siguientes tipos: común o personal. Los *grupos de programas comunes* estarán siempre disponibles en la estación de trabajo, sea cual fuere el usuario que haya iniciado la sesión. Los *grupos de programas personales* son privados del usuario que los crea.

En las estaciones de trabajo con Windows NT, sólo los miembros de los grupos Administradores y Usuarios avanzados podrán crear grupos de programas comunes. Cuando alguno de estos usuarios cree un grupo de programas en una estación de trabajo, podrá especificar si desea que el grupo sea común (es decir, accesible para todos los usuarios de esa estación de trabajo) o personal (accesible únicamente para él). Los grupos de programas personales se guardan como parte del perfil personal y local de un usuario.

Cuando cree perfiles de usuario, sólo podrá incluir grupos de programas personales. Si desea crear un grupo de programas con el fin de incluirlo en el perfil, deberá tratarse de un grupo personal.

Durante la creación de un perfil, también podrá elegir si desea permitir que el usuario de dicho perfil pueda acceder a los grupos de programas comunes de una estación de trabajo. Si decide hacerlo, cuando un usuario inicie una sesión en esa estación de trabajo, aparecerán todos los grupos comunes que existan en la misma y el usuario podrá acceder a ellos. Si opta por ocultar a un usuario los grupos de programas comunes, dicho usuario no podrá ver los grupos comunes en ninguna estación de trabajo. Los únicos grupos de programas que dicho usuario podrá ver serán los grupos personales de su perfil de usuario.

Distintas configuraciones de hardware

Dado que los perfiles que se crean y se asignan a los usuarios pueden utilizarse desde distintos tipos de estaciones de trabajo, conviene tener presente que en dichas estaciones de trabajo pueden existir configuraciones de hardware muy distintas, en particular, distintas tarjetas de vídeo y monitores.

Puesto que un perfil determina la posición y el tamaño de las ventanas en la pantalla, el tipo de adaptador de vídeo existente en la estación de trabajo influye en el funcionamiento del perfil. Por ejemplo, la configuración de ventanas en un perfil que haya sido creado en una computadora (ordenador) con adaptador SuperVGA puede no representarse adecuadamente cuando se cargue en otra computadora con monitor VGA normal.

Para evitar problemas, tenga en cuenta dos cosas:

- Cuando cree o edite un perfil para un usuario individual, utilice una computadora cuyo adaptador de vídeo sea el mismo que el de la computadora que vaya a utilizar habitualmente dicho usuario.
- Cuando cree un perfil obligatorio para un grupo de usuarios, cree un perfil individual para todo el grupo únicamente si todos ellos utilizan computadoras con el mismo tipo de adaptador de vídeo.

  Por ejemplo, si está creando un perfil para un grupo de cajeros del banco, algunos de los cuales utilizan adaptadores SuperVGA y otros adaptadores VGA, lo mejor es crear dos perfiles: CAJERO-SUPERVGA.MAN y CAJERO-VGA.MAN. Cuando lo haga, utilice una computadora con SuperVGA para crear el perfil CAJERO-SUPERVGA.MAN y una computadora con VGA para crear CAJERO_VAG.MAN.

Distintas configuraciones de software

Es probable que en las distintas estaciones de trabajo de su red existan diferentes configuraciones de software. Por ejemplo, puede haber distintas aplicaciones instaladas o éstas pueden encontrarse en distintos lugares. Por este motivo, es posible que las rutas de acceso a los programas especificadas al configurar el Administrador de programas durante la instalación de un perfil de usuario no funcionen en todos los casos. Esto supone un problema especialmente en los casos en que un usuario utilice más de una computadora (ordenador) o cuando se haya establecido un perfil obligatorio para varios usuarios.

A continuación se ofrecen tres posibles soluciones a este problema:

- Poner las aplicaciones necesarias en un servidor y, en la línea de comandos del elemento del grupo de programas, especificar la ruta de acceso correspondiente para cada programa.

  Una ventaja de este método es que facilita la actualización a una nueva versión de un programa para todos los usuarios; basta con actualizar la versión del programa existente en el servidor. Sin embargo, es preciso asegurarse de que se cumplan las posibles restricciones de uso por parte de varios usuarios que establezca la licencia de la aplicación.
- Asegurarse de que la aplicación esté instalada en el mismo lugar en todas las estaciones de trabajo.

  Por ejemplo, si APL.EXE está situada en el directorio C:\EJEMPLO en todas las estaciones de trabajo, no tendrá ningún problema si especifica C:\EJEMPLO\APL.EXE en la línea de comandos de ese elemento de programa.

- Asegurarse de que en la ruta de acceso de búsqueda en todas las estaciones de trabajo aparezca el directorio de aplicación, sea cual sea éste. De este modo, bastará con que especifique el nombre de la aplicación en la línea de comandos correspondiente a su elemento de programa.

  Por ejemplo, si APL.EXE está situada en el directorio C:\EJEMPLO en una computadora y en el directorio D:\APPS\APL en otra, asegúrese de que C:\EJEMPLO aparezca en la ruta de acceso de la primera computadora y D:\APPS\APL en la de la segunda. De este modo, un perfil en el cual se especifique únicamente el nombre del programa (APL.EXE) funcionará en ambas computadoras.

  La ruta de acceso de búsqueda se especifica en el cuadro "Variables de entorno de usuario" de la opción "Sistema" del Panel de control de Windows NT.

Si va a asignar directorios base a los usuarios de su red, puede especificar %HOMEDRIVE%%HOMEPATH% como directorio de trabajo de cada una de las aplicaciones en los perfiles de todos los usuarios. %HOMEDRIVE% y %HOMEPATH% especifican la letra de la unidad local asignada al directorio compartido que contiene el directorio base del usuario y la ruta de acceso a ese directorio, respectivamente. De este modo, cada usuario tendrá un directorio base definido como directorio predeterminado, que se utilizará en todos los cuadros de diálogo del tipo **Abrir** y **Guardar como**.

Uso de perfiles para iniciar aplicaciones automáticamente

Es posible utilizar un perfil para especificar las aplicaciones que se ejecutarán automáticamente cuando el usuario de un perfil inicie una sesión. Para ello, deberá colocar un icono para esa aplicación en un grupo de inicio del usuario.

La mejor forma de crear un grupo de inicio en el perfil de un usuario es por medio del Editor de perfiles de usuario. Esta herramienta permite designar como grupo de inicio cualquiera de los grupos de programas del usuario. Obsérvese que cuando se designa un grupo de inicio de esta manera, no es necesario que dicho grupo tenga el nombre Inicio.

Cuando un usuario inicie una sesión en una estación de trabajo puede que se ejecuten automáticamente las aplicaciones de hasta dos grupos de programas.

1. Si en la estación de trabajo existe un grupo de programas común llamado Inicio, se ejecutarán las aplicaciones de ese grupo.
2. Si el usuario tiene un perfil basado en servidor y se ha utilizado el Editor de perfiles de usuario para designar como grupo de inicio alguno de los grupos de programas del usuario, se iniciarán las aplicaciones de ese grupo. Si el usuario no tiene ningún perfil, o si su perfil no tiene designado ningún grupo de inicio, Windows NT comprobará si el usuario posee algún grupo personal llamado Inicio. Si es así, se ejecutarán las aplicaciones de ese grupo.

   Obsérvese que el grupo personal Inicio de un usuario sólo funcionará si ningún administrador ha designado como grupo de inicio a alguno de los otros grupos de programas del usuario. Si algún administrador lo ha hecho, se desactivará el grupo personal del usuario llamado Inicio.

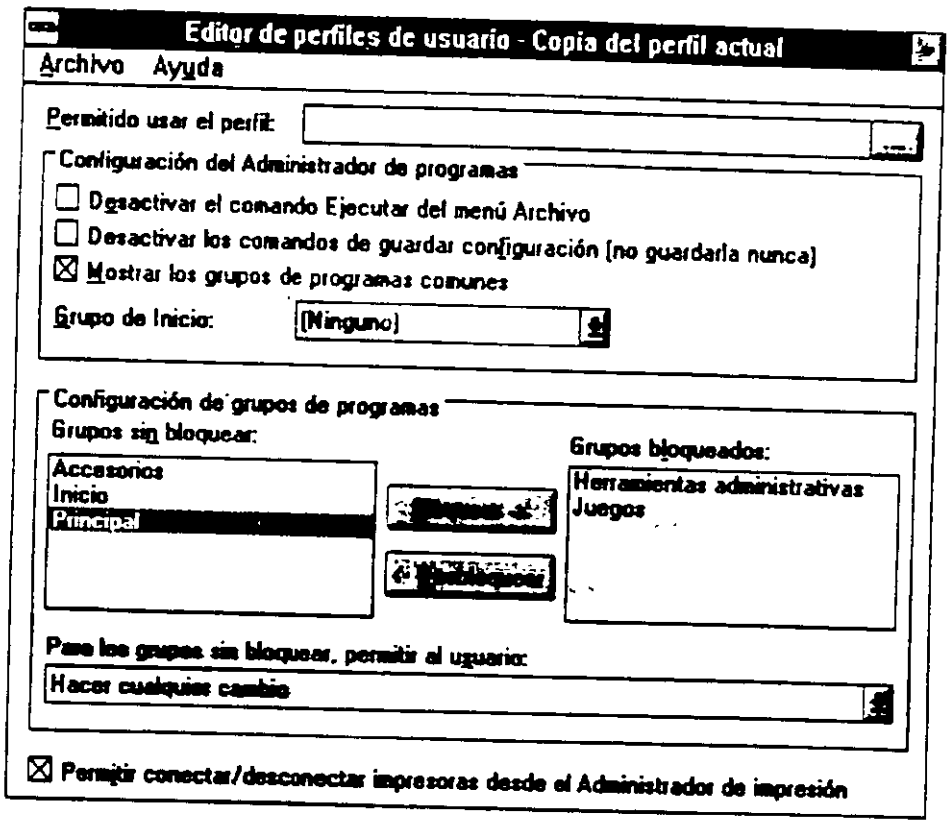
Creación de perfiles de usuario

Puede crear un perfil basado en servidor, de dos diferentes maneras, dependiendo si desea establecer configuraciones iniciales en el perfil.

Si no necesita establecer configuraciones en el perfil, puede especificar un nombre de archivo de perfil personal (con la extensión USR) en cada cuenta de usuario. No debe existir ningún archivo con el mismo nombre de archivo. de esta manera la próxima vez que el usuario inicie una sesión, Windows NT verificará que no existe actualmente un perfil basado en servidor para el usuario. Cuando el usuario cierra la sesión, Windows NT crea un archivo con el nombre de archivo que especificó y guarda todas las configuraciones de cada usuario en el archivo que éste tuviese. Este será el perfil que se cargará la próxima vez que inicie una sesión. Esta es una manera excelente de compartir las ventajas de un perfil basado en servidor con muchos usuarios, aunque estos ya tengan cuentas de usuarios. Asegúrese de especificar un nombre de archivo de perfil diferente para cada usuario, de manera que las modificaciones realizadas por un usuario no afecten a los demás.

Si desea establecer configuraciones en los perfiles de usuario, puede crear el perfil utilizando el Editor de perfil de usuario y seguir los tres pasos siguientes:

1. Acceda a una estación de trabajo con Windows NT y configúrela de la manera deseada. Utilice el Administrador de programas para crear elementos y grupos de programas, establezca las conexiones de red, defina el tamaño y la posición de la ventana, y especifique el aspecto de la pantalla.
2. Utilice el Editor de perfiles de usuario para especificar otras opciones del usuario y, si lo desea, restringir las acciones que el usuario podrá realizar en esa estación de trabajo.



3. Utilice el Editor de perfiles de usuario para conceder a un usuario o grupo los permisos necesarios para utilizar ese perfil, luego guarde el perfil. De este modo se guardarán tanto las opciones seleccionadas mediante el Editor de perfiles de usuario como la configuración general que se creó con el paso 1.

   Cuando guarde un perfil de usuario, podrá almacenarlo como perfil personal o como perfil obligatorio normal, o bien como el perfil predeterminado de sistema o perfil predeterminado de la estación de trabajo. Los perfiles predeterminados se describen en "Concepto de perfil predeterminado", sección anterior de este mismo capítulo. El *perfil predeterminado de sistema* se utilizará en una computadora (ordenador) cuando ningún usuario haya iniciado una sesión en la misma. Las únicas opciones que contempla un perfil de sistema son el papel tapiz, el color de segundo plano y la configuración de protectores de pantalla.

Si desea obtener instrucciones más detalladas, consulte el *Manual de sistema de Microsoft Windows NT Advanced Server*.

Administración de perfiles existentes

Cuando desee modificar un perfil existente, puede utilizar uno de los siguientes procedimientos:

- Asigne el perfil a una cuenta de usuario y posteriormente inicie una sesión en una estación de trabajo, especificando esa cuenta como su nombre de usuario. Luego, modifique el perfil utilizando el Editor de perfiles de usuario o introduciendo cambios en el entorno de usuario con las herramientas normales de Windows, como el Administrador de programas o el Panel de control.
- O bien, abra el Editor de perfiles de usuario y modifique sus opciones. Podrá utilizar este método cuando haya iniciado la sesión utilizando su cuenta de usuario habitual. Sin embargo, sólo podrá modificar aquellas opciones que aparezcan en el Editor de perfil de usuarios; por ejemplo, no podrá crear grupos de programas personales, modificar el tamaño de las ventanas ni cambiar los colores de la pantalla.

Si utiliza el primer método para modificar los perfiles, es conveniente que antes cree una cuenta especial de usuario para utilizarla durante la administración de perfiles. De este modo, cuando desee modificar un perfil, podrá asignar temporalmente dicho perfil a la cuenta del administrador de perfiles, en lugar de asignarlo a su cuenta de usuario.

Para crear una cuenta de administrador de perfiles, cree una cuenta de usuario normal utilizando el Administrador de usuarios y asegúrese de agregar esa cuenta al grupo global Administradores de dominios de ese dominio.

Archivos de comandos de inicio de sesión

Los archivos de comandos de inicio de sesión son archivos por lotes o archivos ejecutables que se procesan automáticamente cada vez que un usuario inicia una sesión en una estacion de trabajo con Windows NT o MS-DOS. Los archivos de comandos de inicio de sesión suelen utilizarse para configurar los entornos de trabajo de los usuarios, estableciendo las conexiones de red necesarias e iniciando aplicaciones.

Los perfiles de usuario permiten no sólo lo mismo que los archivos de comandos de inicio de sesión sino también algunas cosas más. Sin embargo, existen varios casos o motivos por los cuales puede interesar utilizar archivos de comandos de inicio de sesión en lugar de, o además de, los perfiles de usuario:

- Cuando existen usuarios que utilicen estaciones de trabajo con MS-DOS. Los perfiles de usuario sólo funcionan con estaciones de trabajo con Windows NT.
- Cuando se desea administrar una parte de los entornos de los usuarios (por ejemplo, las conexiones de red) sin necesidad de administrar o determinar la totalidad del entorno.
- Si se utilizan únicamente perfiles personales, puede usar archivos de comandos de inicio de sesión para crear conexiones de red comunes para varios usuarios.
- Los archivos de comandos de inicio de sesión son más fáciles de crear y mantener.
- Cuando ya se está ejecutando en la red LAN Manager 2.x y desea seguir utilizando los archivos de comandos de inicio de sesión que fueron creados para ese sistema.

Funcionamiento de los archivos de comandos de inicio de sesión

Para asignar a un usuario un archivo de comandos de inicio de sesión, basta con especificar en la cuenta de usuario la ruta de acceso del archivo de comandos. Una vez hecho esto, cada vez que el usuario inicie una sesión, se cargará y ejecutará su archivo de comandos de inicio de sesión. Es posible asignar un archivo de comandos distinto para cada usuario o crear archivos de comandos comunes para varios de ellos.

Nota La ruta de acceso especificada en la cuenta de usuario es relativa a la ruta de acceso empleada para los archivos de comandos de inicio de sesión en la computadora (ordenador) en la cual esté almacenado el archivo de comandos. Por ejemplo, si la ruta de acceso para los archivos de inicio de sesión de esa computadora es WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS y el archivo de comandos de PaulaS es WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS\PAULAS.BAT, sólo necesitará especificar PAULAS.BAT como ruta de acceso del archivo de comandos de inicio de sesión de la cuenta PaulaS.

Para crear un archivo de comandos por lotes para el inicio de sesión, bastará con que cree un archivo por lotes de MS-DOS. Si desea obtener más información sobre la manera de crear archivos por lotes, consulte el *Manual de sistema de Microsoft Windows NT Advanced Server* o su documentación de MS-DOS.

Existen diversos parámetros especiales que pueden utilizarse durante la creación de archivos de comandos, como muestra la tabla siguiente:

Parámetros especiales de los archivos de comandos de inicio de sesión

Parámetro	Descripción
%HOMEDRIVE%	Letra de unidad de la estación de trabajo local del usuario conectada al directorio base del usuario
%HOMEPATH%	Ruta de acceso completa del directorio base del usuario
%HOMESHARE%	Nombre del directorio compartido que contiene el directorio base del usuario
%OS%	Sistema operativo de la estación de trabajo del usuario
%PROCESSOR%	Tipo de procesador (por ejemplo, 80386) de la estación de trabajo del usuario
%USERDOMAIN%	Dominio que contiene la cuenta del usuario
%USERNAME%	Nombre de usuario correspondiente a ese usuario

Los archivos de comandos de inicio de sesión se cargan siempre desde la computadora que se encarga de validar las peticiones de inicio de sesión de los usuarios. Para aquellos usuarios que posean cuentas en dominios de Windows NT Advanced Server en los cuales existan varios servidores, cualquiera de los servidores del dominio podrá autorizar los intentos de inicio de sesión de un usuario. Por lo tanto, para garantizar que los archivos de comandos de inicio de sesión funcionen para todos los usuarios, asegúrese de que los archivos de comandos de inicio de sesión de todas las cuentas de usuario del dominio existan en todas los servidores con Windows NT Advanced Server del dominio.

La mejor forma de conseguirlo es utilizar el servicio Duplicador. Este servicio mantiene copias idénticas de un árbol de directorios en varias computadoras diferentes. Cuando se realice algún cambio en un archivo de la copia maestra del árbol (que está situada en el *servidor de Exportación*), el servicio Duplicador copiará automáticamente ese cambio en las demás computadoras (las *computadoras importadoras*).

Cuando utilice el servicio Duplicador con archivos de comandos de inicio de sesión, configurará uno de los servidores con Windows NT Advanced Server como servidor de Exportación y todos los demás servidores del dominio como computadoras importadoras.

Si desea obtener más información sobre el servicio Duplicador, consulte el capítulo 5, "Administración de archivos de la red". Si desea obtener instrucciones sobre la manera de configurar y utilizar el servicio Duplicador, consulte el *Manual de sistema de Windows NT Advanced Server*.

Directorios base

Los directorios base pueden servir como áreas de almacenamiento privado para los usuarios. Normalmente, los usuarios utilizarán sus directorios base para almacenar datos privados. Por lo general, un usuario también podrá controlar el acceso a su directorio base y restringir o conceder el acceso al mismo por otros usuarios.

Si en las estaciones de trabajo de su red hay poco espacio libre en disco duro, puede que le interese asignar a cada usuario un directorio base situado en un servidor. También es posible asignar a los usuarios directorios base situados en sus propias estaciones de trabajo; por ejemplo, puede hacerlo si en la estación de trabajo de un usuario existe espacio suficiente en disco duro para almacenar los datos del usuario, pero no desea que dicho usuario pueda acceder a los demás archivos y directorios de la estación de trabajo. En este caso, probablemente lo que habrá que hacer es configurar la estación de trabajo del usuario de tal modo que su directorio base, así como los subdirectorios que contiene, sean los únicos para los cuales el usuario disponga de permisos superiores a Listado. Si desea obtener más información sobre los permisos de archivos y directorios, consulte el capítulo 5, "Administración de archivos de la red".

Si un usuario posee un directorio base en una computadora distinta de la suya, se establecerá automáticamente una conexión con el directorio base cada vez que dicho usuario inicie una sesión.

Cada vez que un usuario inicie una interfaz de comandos, se seleccionará como directorio predeterminado el directorio base de ese usuario. Este directorio base del usuario también quedará seleccionado como directorio de trabajo en todas las aplicaciones que inicie el usuario, excepto en aquéllas para las cuales exista un elemento de programa que especifique un directorio de trabajo distinto.

Windows NT proporciona tres parámetros reemplazables, que pueden sustituirse para utilizarlos con los directorios base: %HOMEPATH%, %HOMEDRIVE% y %HOMESHARE%. %HOMEPATH% representa el nombre de la ruta de acceso del directorio base del usuario; %HOMEDRIVE% es la letra de unidad local necesaria para la conexión de red con el directorio base, en caso de que dicho directorio no esté situado en la propia estación de trabajo del usuario; %HOMESHARE% es el nombre según UNC (convención de nomenclatura universal) del directorio compartido que contiene el directorio base del usuario. Puede utilizar estas variables cuando instale archivos de comandos de inicio de sesión u otros archivos por lotes, o desde el Administrador de programas; por ejemplo, cuando especifique rutas de acceso de aplicaciones o directorios de trabajo.

Configuración de las variables de entorno

En una computadora (ordenador) con Windows NT, las *variables de entorno* son opciones diversas que influyen sobre el modo en que Windows NT encuentra los programas, asigna espacio de memoria para determinados programas y controla el comportamiento de otros.

Windows NT dispone de dos tipos de variables de entorno: de usuario y de sistema. La opción "Sistema" del Panel de control permite ver tanto las variables de entorno de usuario como las de sistema.

Las variables de entorno de usuario pueden ser distintas para cada uno de los usuarios de una estación de trabajo. Puede utilizarse esta opción del Panel de control para cambiar los valores de las variables de entorno de usuario y crear otras nuevas.

Las variables de entorno de sistema de una computadora serán las mismas para todos los usuarios de esa computadora. Son definidas por Windows NT, y no puede utilizarse la opción "Sistema" para agregar nuevas variables de entorno de sistema ni para modificar los valores de las mismas.

Sin embargo, aunque no está permitido cambiar directamente los valores de las variables de entorno de sistema, sí es posible sobrescribirlas, creando variables de entorno de usuario con nombres idénticos a los de las variables de entorno de sistema que se desee sobrescribir. Si existe algún conflicto entre variables de entorno, Windows NT lo resolverá del siguiente modo:

1. Primero se configuran las variables de entorno de sistema.
2. A continuación se configuran las variables definidas en el cuadro de diálogo **Sistema**.
3. Por último se configuran las variables de entorno definidas en AUTOEXEC.BAT.

Si se configura una variable de entorno como una variable de entorno de sistema y como variable de entorno de usuario, el valor de esta última anula el valor de la primera. Sin embargo, las variables en AUTOEXEC.BAT no anulan los otros dos tipos de variables de entorno. Si una variable de AUTOEXEC.BAT duplica a otra variable, el valor de AUTOEXEC.BAT será descartado.

La variable de entorno PATH es una excepción a esta regla. Los directorios especificados en la variable de entorno de usuario PATH y AUTOEXEC.BAT se agregarán a los que se hayan especificado en la variable de entorno de sistema PATH.

Las variables de entorno de usuario se guardan en los perfiles de usuario.

En las siguientes tablas se muestran las variables de entorno de usuario y de sistema disponibles. También es posible agregar nuevas variables de entorno de usuario.

Variables de entorno	Explicación
Sistema:	
ComSpec	Especifica el directorio en el cual está situado el intérpre de comandos, CMD.EXE.
OS2LibPath	Especifica los directorios en los cuales los programas que se ejecuten con el subsistema OS/2 deberán buscar los archivos .DLL.
Path	Especifica los directorios en los cuales deberán buscarse los archivos de programas ejecutables.
WinDir	Especifica el directorio en el cual está instalado Windows NT o Windows NT Advanced Server. Esta variable se incluye para garantizar la compatibilidad descendente de aplicaciones más antiguas.
Usuario:	
tmp temp	Estas dos variables especifican el directorio predeterminado en el cual las aplicaciones podrán guardar los archivos temporales durante su ejecución. Son necesarias ambas variables porque algunas aplicaciones existentes utilizan **tmp** como variable de entorno, mientras que otras emplean **temp**.

Ejemplos de variables de entorno de usuario

En la siguiente sección se ofrecen algunos casos ficticios que ilustran la forma en que deben aplicarse los conceptos explicados en este capítulo.

Configuración de entornos de usuario fáciles de usar

Supongamos que se desea configurar entornos de usuario de tal modo que resulten fáciles de utilizar para un grupo de usuarios de Windows NT que necesiten el mismo conjunto de conexiones iniciales de red y elementos de programa.

Para poder modificar los elementos de programa, deberá utilizar perfiles. Puede utilizar perfiles obligatorios o perfiles personales. Para decidir qué perfiles utilizar, piense en cómo desea que se modifiquen y mantengan los perfiles. Si desea poder modificar el entorno de todo el grupo de usuarios a la vez, utilice perfiles obligatorios. Si desea que los usuarios puedan realizar cambios duraderos en sus propios entornos, utilice perfiles personales.

Cuando lo haya decidido, cree una cuenta de usuario y asígnele el nombre Administrador de perfiles. Inicie una sesión con esta cuenta. Luego establezca las conexiones de red que desee que se realicen automáticamente cuando los usuarios inicien una sesión y cree elementos de programa para las aplicaciones que necesitan. Configure también todas las demás opciones del entorno, que desee que posean los usuarios. A continuación, inicie el Editor de perfiles de usuario y guarde la configuración como un perfil. Si ha decidido utilizar perfiles obligatorios, asigne al perfil un nombre que represente al grupo y utilice la extensión .MAN (por ejemplo, CONTABLE.MAN). Si está utilizando perfiles personales, asigne al perfil un nombre de archivo idéntico al nombre de uno de sus usuarios y utilice la extensión .USR (por ejemplo, PEDROT.USR).

Cierre la sesión con la cuenta Administrador de perfiles e inicie otra sesión con su cuenta de administración habitual.

Utilice el Administrador de usuarios para asignar el perfil a las correspondientes cuentas de usuario. Si ha optado por utilizar un perfil obligatorio, su trabajo habrá terminado.

Si optó por utilizar perfiles personales y aún no ha creado las cuentas de usuario de todos los usuarios que vayan a emplear ese perfil, deberá hacerlo ahora, copiando la cuenta de usuario a la cual asignó este primer perfil. De este modo, la configuración del nombre de perfil correspondiente a la nueva cuenta se realizará automáticamente. Por ejemplo, si creó una cuenta JuanG copiando la cuenta PedroT y en la cuenta PedroT especificó como perfil de usuario personal PEDROT.USR, el nombre del perfil de usuario de la cuenta JuanG pasará a ser automáticamente JUANG.USR.

Para terminar el trabajo necesario para configurar los perfiles personales, copie varias veces el perfil original que creó (copiándolo con un nuevo nombre de archivo cada vez) hasta que exista un archivo de perfil para cada uno de los usuarios. El nombre de archivo de cada perfil debe coincidir con el nombre de usuario del usuario al que corresponda: por ejemplo, si ErnestoA es uno de los usuarios, deberá copiar el perfil en un archivo llamado ERNESTOA.USR.

Si en las cuentas de usuario de cada uno de los usuarios no está ya especificado el correspondiente nombre de archivo, utilice el Administrador de archivos para hacerlo.

Administración de archivos de la red

Uno de los usos más importantes de los servidores, en la mayoría de las redes, es compartir archivos y directorios con otros usuarios de la red. Cuando un directorio está compartido, los usuarios pueden conectarse a él desde sus propias estaciones de trabajo y acceder desde ellas a los archivos que contenga el directorio. El directorio compartido funciona como si fuera otro disco duro que pueden utilizar los usuarios.

El sistema operativo Windows NT Advanced Server ofrece un rendimiento excelente, fiabilidad y seguridad para compartir archivos, en especial cuando se utiliza el sistema de archivos de Windows NT (NTFS).

Puede establecer *permisos de archivos* en los directorios y en los archivos de los volúmenes NTFS, de manera que únicamente puedan acceder a ellos los usuarios que especifique. Con los permisos de archivos en NTFS, puede establecer una seguridad diferente para cada archivo y cada directorio. Para cada uno de ellos puede especificar exactamente qué grupos y qué usuarios podrán acceder a los archivos, y el nivel de acceso que tiene permitido cada grupo o cada usuario. Los permisos de archivos en NTFS se aplican a los usuarios que trabajan en la computadora (ordenador) que contiene los archivos y a los usuarios que accedan a ellos a través de la red (si están compartidos).

Puede *auditar* el acceso a los archivos y directorios de los volúmenes NTFS del servidor. Si lo hace, siempre que un usuario acceda a un archivo, se escribirá una entrada en el registro de seguridad de los servidores que estén ejecutando Windows NT Advanced Server. Puede definir exactamente qué tipos de acceso para cada archivo o directorio realizarán la escritura de una entrada.

También se utiliza el concepto de *posesión de archivo*. Cada archivo y cada directorio tienen un propietario que controla el acceso al archivo o al directorio. Los demás usuarios únicamente podrán acceder a él si lo permite el propietario.

Windows NT Advanced Server también admite la duplicación de directorios. Mediante el servicio Duplicador podrá configurar el árbol de directorios de un servidor (denominado servidor de Exportación), y designar otros servidores y estaciones de trabajo (denominados computadoras importadoras) para que mantengan duplicados de este árbol de directorios. Posteriormente, si realiza cambios en el árbol de directorios del servidor de Exportación, Windows NT Advanced Server copiará los archivos modificados a todas las computadoras (ordenadores) importadoras, con la seguridad de que todas ellas tendrán siempre copias idénticas del árbol.

Nota Tanto los servidores que ejecutan Windows NT Advanced Server como las estaciones de trabajo con Windows NT pueden compartir archivos con los usuarios de la red. Puesto que este manual está dirigido a los administradores de redes con Windows NT Advanced Server, se ha escrito suponiendo que comparte archivos utilizando servidores que ejecuten Windows NT Advanced Server. No obstante, tenga presente que todas las técnicas para compartir los archivos mencionadas en este capítulo también pueden ser utilizadas en las computadoras con Windows NT (con excepción de configurar la computadora como servidor de Exportación para el servicio Duplicador).

Elección de un sistema de archivos

Los servidores que ejecuten Windows NT Advanced Server admiten tres sistemas de archivos: el sistema de archivos de Windows NT (NTFS), el sistema de archivos de tabla de asignación de archivos (FAT) y el sistema de archivos de alto rendimiento (HPFS).

Un servidor que ejecute Windows NT Advanced Server puede utilizar uno o más de estos sistemas de archivos en sus discos y particiones. En cada uno de los servidores es necesario elegir el sistema o los sistemas que desee utilizar en cada uno de los servidores.

Se recomienda tener en cuenta las siguientes directrices para elegir el sistema o los sistemas de archivos:

1. Si el servidor no necesita cargar inicialmente MS-DOS u OS/2 además de Windows NT Advanced Server, utilice en el servidor únicamente el sistema NTFS.
2. Si el servidor necesita cargar inicialmente MS-DOS u OS/2, mantenga el sistema de archivos actual (MS-DOS o HPFS) en la unidad C. Opcionalmente, puede utilizar el sistema NTFS en particiones adicionales del servidor, siempre y cuando MS-DOS u OS/2 no necesiten leer dichas particiones.

Las siguientes directrices adicionales pueden afectar su decisión en cuanto al sistema o sistemas de archivos que desee utilizar en sus servidores.

- En una computadora (ordenador) tipo x86, Windows NT buscará durante el inicio determinados archivos en el directorio raíz de la unidad C. Por lo tanto, esta partición deberá tener el formato de uno de los sistemas de archivos mencionados (NTFS, HPFS o FAT) y deberá tener un tamaño suficientemente grande como para acomodar todos los archivos a los que necesite acceder bajo ese sistema de archivos.
- En una computadora tipo RISC, la partición de sistema debe tener el formato del sistema de archivos FAT. Si desea utilizar el sistema NTFS, debe crear una segunda partición de un tamaño suficiente como para que contenga todos aquellos archivos que desee proteger con la seguridad de Windows NT.

En la siguiente tabla se describen las ventajas y desventajas de cada uno de estos tres sistemas.

Ventajas y desventajas de cada sistema de archivos

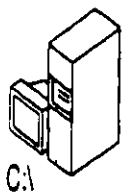
Ventajas	Desventajas
Sistema de archivos de Windows NT (NTFS):	
Admite la seguridad completa de Windows NT, de manera que pueda especificar quién tiene permitido varios tipos de acceso a un archivo o a un directorio. Este "control de acceso discrecional" está disponible para los archivos de las particiones NTFS.	Unicamente reconocido por Windows NT. Cuando la computadora (ordenador) está ejecutando otro sistema operativo (como MS-DOS u OS/2), éste no podrá acceder a los archivos de la partición NTFS.
Mantiene un registro de las actividades para restaurar un disco en caso de corte del suministro eléctrico u otros problemas.	Si la unidad C tiene el formato del sistema NTFS, no podrá ejecutar MS-DOS desde el disco duro (pero sí podrá ejecutar aplicaciones basadas en MS-DOS).
Admite las funciones de tolerancia a fallos de Windows NT.	
Admite nombres de archivos y directorios de hasta 256 caracteres, así como atributos de archivos extendidos. Genera automáticamente nombres de archivo de MS-DOS correctos, de modo que los archivos puedan compartirse con usuarios de MS-DOS.	
Un programa que esté concebido para ejecutarse bajo otros sistemas operativos, como MS-DOS, puede acceder a los archivos del sistema NTFS cuando se ejecute bajo Windows NT.	
En una computadora con Windows NT, NTFS proporciona mayores características que los sistemas FAT o HPFS.	

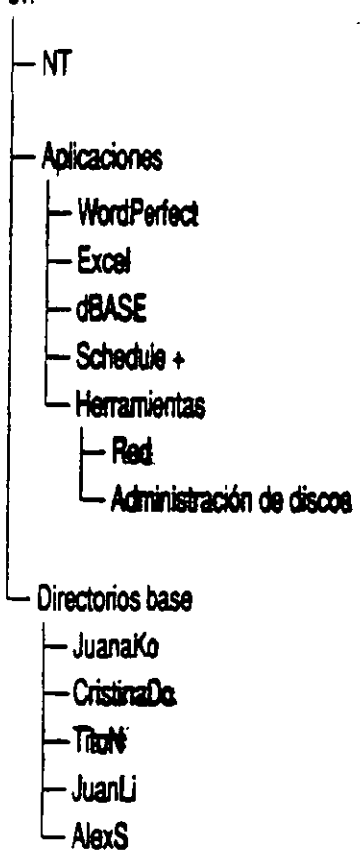
ntajas y desventajas de cada sistema de archivos

Ventajas	Desventajas
Tabla de asignación de archivos (FAT):	
Puesto que es el sistema de archivos de uso más extendido para PC, puede accederse a los archivos cuando se esté ejecutando otro sistema operativo en la computadora (por ejemplo, MS-DOS u OS/2).	Los archivos de una partición FAT no están protegidos por las características de seguridad de Windows NT.
Debe utilizar el sistema FAT en la partición de la unidad C si desea ejecutar MS-DOS desde el disco duro. Los disquetes o los discos duros extraíbles que utilice para compartir archivos entre computadoras deben utilizar el sistema FAT.	Los nombres de los archivos de una partición FAT tienen una restricción de 8 caracteres para el nombre y 3 caracteres para la extensión.
	No admite archivos de gran tamaño.
	Menos completo que el sistema NTFS; por ejemplo, no dispone de características de restauración automática de discos.
Sistema de archivos de alto rendimiento (HPFS):	
Creado para la versión 1.2 o superior del sistema operativo OS/2, y utilizado por este sistema.	No tiene un uso extendido.
Admite nombres largos para los archivos.	Los archivos de una partición HPFS no están protegidos por la seguridad de Windows NT.
Proporciona una corrección de errores mejor que la del sistema FAT.	En los volúmenes HPFS, las aplicaciones basadas en MS-DOS y en Windows 3.1 no pueden acceder a los archivos o directorios que tengan nombres largos en su ruta de acceso.

Compartir archivos con los usuarios de la red

Cuando comparte un directorio del servidor, los usuarios pueden teóricamente acceder a ese directorio y a los archivos que contenga, a todos sus subdirectorios y a los archivos que contengan, a todos los subdirectorios de dichos subdirectorios y a los archivos que contengan, etc. Todo punto del árbol de directorios situado debajo del directorio compartido puede estar disponible para los usuarios de la red.





Cuando se comparte un directorio, los subdirectorios también están disponibles en la red.

Sin embargo, si el directorio compartido está en una partición NTFS, podrá bloquear el acceso a algunos de los directorios de un árbol de directorios compartido y, a la vez, permitir el acceso a otros directorios, estableciendo permisos para los distintos directorios. Por ejemplo, en la figura anterior, podría compartir el directorio Aplicaciones pero definir los permisos de modo que los usuarios puedan acceder a todos los directorios situados debajo de él excepto a dBASE®.

Cuando comparte un directorio, debe asignarle un *nombre compartido*, es decir, un nombre que deberán utilizar los usuarios de la red para referirse a ese directorio. Los usuarios de Windows verán el nombre compartido cuando utilicen el Administrador de archivos para examinar la red y los usuarios de MS-DOS podrán ver el nombre compartido cuando utilicen el comando **net view**. Un nombre compartido puede ser el mismo que el nombre real del directorio, aunque también puede ser distinto.

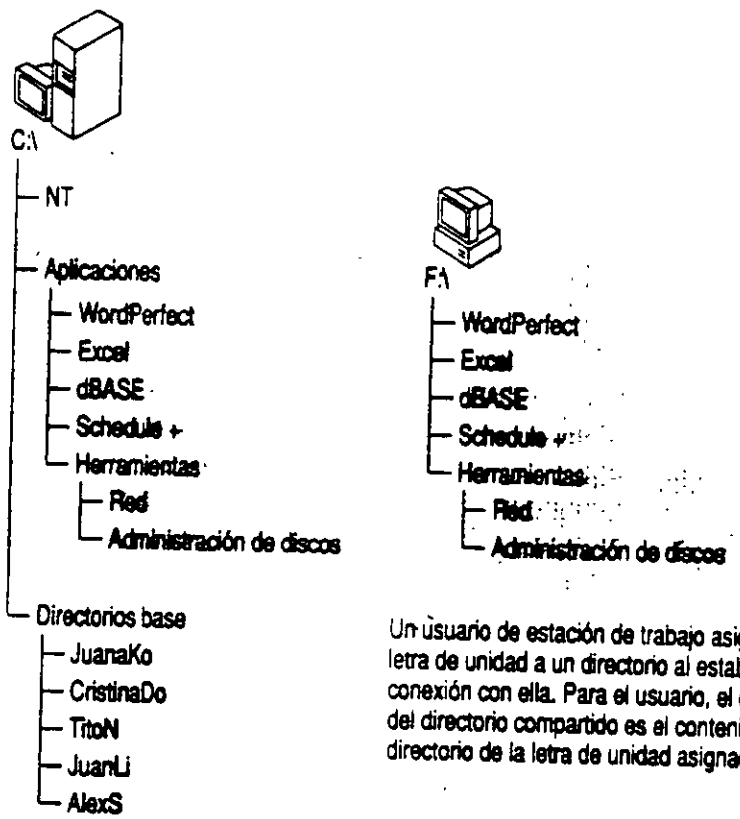
Los usuarios verán el nombre compartido agregado al nombre de la computadora (ordenador) del servidor. Por ejemplo, si comparte un directorio en el servidor Producción y asigna al directorio el nombre compartido Datos, los usuarios verán el recurso compartido como PRODUCCION\DATOS.

Un directorio compartido se denomina a veces *recurso compartido*.

Si lo desea, puede compartir varios directorios en el mismo árbol de directorios. En este caso, los usuarios podrían acceder a un directorio compartido de dos maneras: como uno de los directorios realmente compartido y como un subdirectorio de otro directorio compartido.

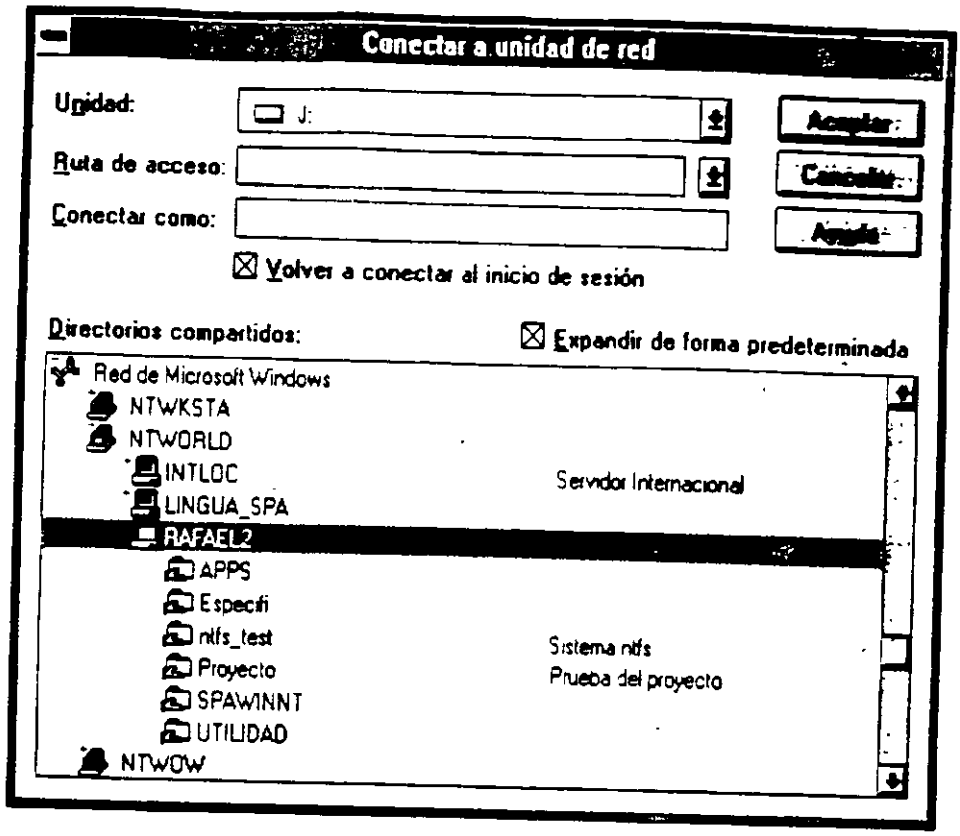
Conexión de los usuarios

Los usuarios de la red generalmente se conectan con los directorios compartidos asignando una letra de unidad a dichos directorios en su estación de trabajo. Después utilizan esta letra de unidad para hacer referencia al directorio con el que estén conectados. Por ejemplo, supongamos que un usuario se ha conectado al directorio Aplicaciones de la figura siguiente y ha asignado al directorio la letra de unidad F:. Este usuario verá el contenido del directorio Aplicaciones del servidor como si fuera el contenido de su unidad F. Para él, el subdirectorio HERRAMIENTAS será F:\HERRAMIENTAS.



Un usuario de estación de trabajo asigna una letra de unidad a un directorio al establecer una conexión con ella. Para el usuario, el contenido del directorio compartido es el contenido del directorio de la letra de unidad asignada.

Los usuarios de Windows NT, Windows para Trabajo en grupo y Windows 3.1 utilizan el Administrador de archivos para efectuar conexiones a través de la red, usando un cuadro de diálogo similar al siguiente (el cuadro de diálogo exacto dependerá del sistema que esté ejecutando el usuario).



Cuando un usuario de Windows se conecte a un directorio, podrá ver la letra de unidad que haya asignado al directorio y aparecerá un icono en la barra de unidades del Administrador de archivos.

Los usuarios de computadoras (ordenadores) con MS-DOS que estén ejecutando software de estaciones de trabajo con LAN Manager (pero sin Windows) deberán utilizar el comando **net use** para conectarse a través de la red. El comando siguiente conecta la letra de unidad F: del usuario al directorio HERRAMIENTAS, del servidor denominado PRODUCCION.

```
net use f: \\producción\herramientas
```

Los usuarios de estaciones de trabajo con MS-DOS (con y sin Windows 3.1 o Windows para Trabajo en grupo) tienen restricciones adicionales sobre la manera de ver y acceder a los directorios compartidos, como se describe en la siguiente sección.

Consideraciones para los usuarios de MS-DOS

Cuando asigne nombres compartidos a los directorios compartidos, tenga en cuenta si deben acceder a ellos usuarios de MS-DOS (incluyendo usuarios de Windows 3.1 y de Windows para Trabajo en grupo). En ese caso, asigne un nombre que cumpla la convención de nombres de 8.3 de MS-DOS, donde el nombre puede tener hasta 8 caracteres, seguido de un punto y, opcionalmente, de hasta 3 caracteres. Los usuarios de las estaciones de trabajo con MS-DOS no podrán ver ni acceder a los directorios compartidos cuyos nombres no cumplan esta convención.

Si a un directorio compartido únicamente van a acceder usuarios de Windows NT, podrá utilizar un estilo diferente para los nombres compartidos, que podrán tener hasta 12 caracteres.

En los volúmenes NTFS puede asignar nombres de archivos y directorios de hasta 255 caracteres. No obstante, no necesita preocuparse de si estos nombres serán vistos por usuarios de MS-DOS. El sistema NTFS proporciona mapeados de nombres, donde cada archivo o cada directorio cuyo nombre no cumpla la norma 8.3 de MS-DOS recibe automáticamente un nombre que sí la cumple. Los usuarios de MS-DOS que accedan al archivo o al directorio a través de la red verán el nombre en el formato 8.3, pero los usuarios de Windows NT seguirán viendo el nombre largo. Tenga en cuenta que el sistema NTFS solamente crea nombres cortos para los archivos y directorios que tengan nombres largos. No genera nombres cortos para los nombres compartidos que no cumplan con las normas de asignación de nombres de MS-DOS.

Los mapeados de nombres de Windows NT permiten además que las aplicaciones que no admiten nombres largos puedan acceder a los archivos con esos nombres. Estas aplicaciones hacen referencia a archivos con nombre largo por su nombre más corto.

Nota Si una aplicación que no admite nombres largos abre un archivo con un nombre largo y después lo guarda, se pierde el nombre largo y únicamente se conserva el nombre corto.

Cuando cree un nombre largo, Windows NT utilizará las siguientes reglas para generar un nombre corto:

- Los espacios en blanco se eliminan.
- Los caracteres que no están permitidos en los nombres de MS-DOS se cambian por signos de subrayado (_).
- El nombre se trunca detrás del sexto carácter (o delante del primer punto del nombre largo si está entre los seis primeros caracteres); después se agregan un guión y un número a estos seis caracteres. El número para el primer nombre corto creado para un conjunto de seis caracteres es un 1. Si se crean más nombres empleando estos seis caracteres, el siguiente nombre corto utilizará un 2, etc. Si crea un décimo nombre, sólo se utilizarán cinco caracteres del nombre largo y se agregará un 10 a continuación del guión.
- Si el nombre largo contiene algún punto seguido por otros caracteres, el último de los puntos y los 3 primeros caracteres que le sigan se utilizarán como la extensión del nombre corto. Por ejemplo, el nombre corto correspondiente a DOCS.MUY.IMPORTANTES será DOCS~1.IMP.

Si utiliza Windows NT Advanced Server en un entorno en el que no siempre se admiten los nombres largos, podría ser conveniente seguir utilizando las convenciones de MS-DOS para los 6 primeros caracteres de los nombres y utilizar puntos únicamente para separar los nombres de las extensiones. Por ejemplo, podría dar a un archivo el nombre AGOVEN~Agosto 1992 Informe de ventas.XLS. El nombre corto correspondiente sería AGOVEN~1.XLS.

Uso de permisos para mantener la seguridad de los directorios compartidos

Puede mantener la seguridad de los directorios compartidos, asegurándose de que únicamente los usuarios autorizados puedan acceder a cada archivo o directorio, y de que estos usuarios sólo puedan acceder a ellos correctamente.

Los permisos no funcionan igual en los volúmenes NTFS que en los volúmenes FAT y HPFS. En los primeros, la seguridad es mucho más completa, podrá establecer permisos diferentes para cada archivo y cada directorio, y estos permisos son aplicables a los usuarios que trabajan en el propio servidor, así como a los usuarios que accedan al directorio a través de la red.

En los volúmenes FAT y HPFS, se concede únicamente un conjunto de permisos para cada directorio compartido, que debe aplicarse a todos los archivos y subdirectorios que contenga el directorio compartido. Además, en los volúmenes FAT y HPFS, los permisos que defina para un directorio compartido no serán aplicables a los usuarios que trabajen en el propio servidor.

Diferencias entre los sistemas de archivos

Función	NTFS	FAT y HPFS
Definir permisos individualmente para cada archivo y cada directorio	Sí	No
Los permisos son aplicables a los usuarios locales	Sí	No
Definir permisos compartidos en los directorios compartidos	Sí	Sí

Nota De manera predeterminada, únicamente los Administradores, Operadores de servidores, Operadores de cuentas, Operadores de impresión y Operadores de copia de seguridad pueden iniciar una sesión localmente en un servidor. Por lo tanto, los archivos de los volúmenes FAT y HPFS de un servidor están protegidos contra el acceso local por parte de los usuarios que no sean miembros de uno de estos grupos, ya que no podrán iniciar una sesión en el servidor.

Funcionamiento de los permisos de archivos en los volúmenes NTFS

Windows NT ofrece un conjunto de *permisos estándar* que pueden definirse para los archivos y directorios de los volúmenes NTFS. Dichos permisos ofrecen combinaciones útiles de tipos específicos de acceso, que se denominan *permisos individuales.*

En las tablas siguientes se muestran los permisos estándar para los directorios y archivos, así como sus significados y qué permiso individual representa cada uno de los permisos estándar. En la primera columna de la primera tabla (bajo permiso de directorio), el primer conjunto de permisos individuales se aplica a los permisos individuales del propio directorio y el segundo a los archivos nuevos que se creen posteriormente en el directorio.

Permisos estándar para directorios y archivos NTFS

Permisos	Significado
Directorio:	
Sin acceso (Ninguno) (Ninguno)	El usuario no puede acceder al directorio de modo alguno, incluso aunque sea miembro de un grupo que tenga asignado permiso de acceso al directorio.
Listado (LC) (Ninguno)	El usuario únicamente puede ver la lista de archivos y subdirectorios de este directorio, y cambiar a un subdirectorio del mismo, pero no puede acceder a los nuevos archivos que se creen en este directorio.
Lectura (LC) (LC)	El usuario puede leer el contenido de los archivos de este directorio y ejecutar aplicaciones que contenga el directorio.
Adición (SC) (Ninguno)	El usuario puede agregar archivos al directorio, pero no puede leer el contenido de los archivos actuales ni cambiarlos.
Adición y lectura (LSC) (LC)	El usuario puede agregar archivos al directorio y leer los archivos actuales, pero no puede modificar archivos.
Cambio (LSCE) (LSC)	El usuario puede leer y agregar archivos, además de modificar el contenido de los archivos actuales.
Control total (Todos) (Todos)	El usuario puede leer y modificar archivos, agregar archivos nuevos, cambiar los permisos del directorio y sus archivos, además de ser propietario del directorio y sus archivos.

Permisos estándar para directorios y archivos NTFS

Permisos	Significado
Archivo:	
Sin acceso	El usuario no puede acceder al archivo de modo alguno, incluso aunque sea miembro de un grupo que tenga asignado permiso de acceso al él.
Lectura (LC)	El usuario puede leer el contenido del archivo y ejecutarlo si es una aplicación.
Cambio (LSCE)	El usuario puede leer, modificar y eliminar el archivo.
Control total (Todos)	El usuario puede leer, modificar, eliminar, establecer permisos para y tomar poseción de un archivo.

Los permisos individuales y sus abreviaturas son:

Lectura (L)	Escritura (S)	Ejecución (C)
Eliminar (E)	Cambio de permisos (M)	Tomar posesión (T)

Si lo desea, puede especificar directamente los permisos individuales cuando defina los permisos de un archivo o de un directorio (en lugar de utilizar los permisos estándar). No obstante, serán raras las ocasiones en que necesite hacerlo (o quizás nunca).

Para trabajar de forma eficaz con la seguridad de NTFS, tenga en cuenta lo siguiente:

- No es necesario asignar Sin acceso, a todos los usuarios, o a todos los grupos que no deban acceder a un archivo o un directorio. Un usuario (o un grupo del que sea miembro el usuario) no podrá acceder a un archivo o a un directorio si no tiene permisos para hacerlo.
- Los permisos son acumulativos. Por ejemplo, si el grupo Colaboradores tiene el permiso Adición para un archivo, el grupo Finanzas tiene el permiso Lectura para el mismo archivo, y si Ana es miembro de ambos grupos, tendrá los permisos Adición y Lectura.

  La excepción es Sin acceso, que tiene prioridad sobre todos los demás permisos. Podrá utilizar este permiso para permitir que un grupo acceda a un archivo al mismo tiempo que impide el acceso de un subgrupo o de una persona miembro de ese mismo grupo. Por ejemplo, supongamos que Ana es miembro del grupo Colaboradores y que tiene el permiso Cambio para un archivo. Si asigna a Ana el permiso Sin acceso para el archivo, Ana no podrá utilizar el archivo aunque sea miembro de un grupo que sí puede acceder a él.

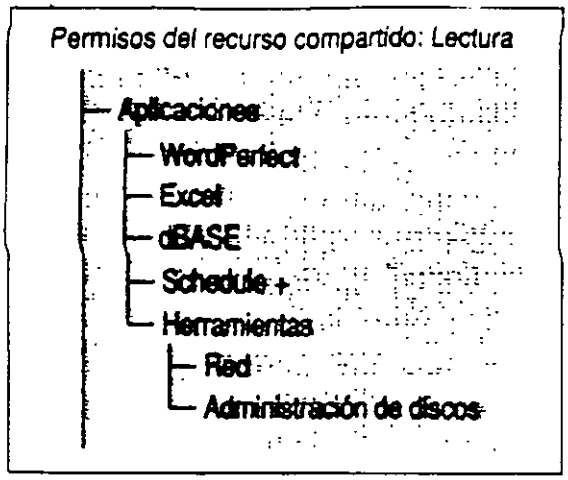
- De manera predeterminada, los archivos y subdirectorios nuevos heredan los permisos del directorio en el que hayan sido creados. Por ejemplo, si agrega un archivo a un directorio para el cual el grupo Colaboradores tiene el permiso Cambio y el grupo Finanzas tiene el permiso Lectura, el archivo tendrá estos mismos permisos.
- Cuando cambie los permisos de un directorio, éstos se aplicarán a todos los archivos que contenga. También existe la posibilidad de elegir si desea aplicar los cambios a todos sus subdirectorios.
- El usuario que cree un archivo o un directorio será su propietario. El propietario de un archivo o un directorio puede controlar el acceso a ellos, cambiando los permisos que tenga definidos. Para obtener más información acerca de la posesión de archivos, consulte "Toma de posesión de archivos", más adelante en este capítulo.

Permisos de recursos compartidos en directorios NTFS compartidos

Antes de compartir un directorio en un volumen NTFS deberá definir los permisos del directorio, y de sus archivos y subdirectorios.

Cuando comparta realmente el directorio, tendrá la oportunidad de definir permisos de recursos compartidos. Estos son adicionales a los permisos individuales de los archivos y directorios. Los permisos de recursos compartidos cumplen la función de un conjunto máximo de permisos para cualquier archivo o subdirectorio del directorio compartido.

Por ejemplo, supongamos que JuanLo tiene el permiso Control total para el directorio APLICACIONES y su subdirectorio HERRAMIENTAS. Después, Ud. comparte el directorio y concede a JuanLo el permiso Lectura de archivos/directorios. Cuando JuanLo acceda a este directorio a través de la red, únicamente podrá leer los archivos. Las restricciones establecidas por los permisos de recursos compartidos impiden a JuanLo el Control total, a pesar de que tiene este permiso para los mismos directorios.



Los permisos establecidos en un recurso compartido limitan a los usuarios el uso de los subdirectorios de dicho recurso. En este ejemplo, JuanLo sólo puede leer el directorio Herramientas a través de la red, debido a las restricciones establecidas por los permisos del recurso compartido.

En el ejemplo anterior, si JuanLo pudiera iniciar la sesión en el propio servidor, tendría Control total para ambos directorios. Los permisos de recursos compartidos se aplican únicamente a los usuarios que accedan a través de la red.

Para simplificar las tareas administrativas, podría definir el permiso de recurso compartido Control total de archivos/directorios siempre que comparta un directorio NTFS (suponiendo que haya decidido bien y con mucho cuidado los permisos que deba asignar a los archivos y directorios individuales del servidor). Al definir el permiso de recurso compartido Control total, está permitiendo en la práctica que los permisos establecidos para los archivos y directorios individuales actúen como medios de seguridad para ellos.

Sin embargo, cuando comparta directorios FAT y HPFS, los permisos de recursos compartidos le proporcionarán un inmejorable medio de control.

Otorgamiento de permisos

Cuando conceda permisos para archivos y directorios en un servidor en el que se esté ejecutando Windows NT Advanced Server, podrá otorgarlos a los siguientes:

- Grupos locales, grupos globales y usuarios individuales del dominio que contenga al servidor
- Grupos globales y usuarios individuales de los dominios en que confíe este dominio
- Los identificadores especiales Todos, SISTEMA, RED, INTERACTIVO y CREADOR PROPIETARIO

Puede conceder permisos a los grupos locales incorporados al dominio (tales como Administradores y Usuarios de dominio) y a cualquier grupo que cree en el dominio.

El identificador especial Todos, representa a todos los usuarios actuales y futuros de la red, incluyendo a los invitados y usuarios de otros dominios. Puede asignar a Todos permisos para acceder tanto a directorios como a archivos.

El SISTEMA representa el sistema operativo de la computadora (ordenador) local. Cuando se instala Windows NT o Windows NT Advanced Server éste tiene permiso de acceso inicial a algunos directorios de sistema. No revoque estos permisos. Por lo general, no es necesario dar permiso al SISTEMA para acceder a los archivos o directorios que cree, a no ser que un servicio del sistema necesite accederlos.

RED representa a todos los usuarios actuales y futuros que accedan al archivo, o al directorio a través de la red. INTERACTIVO es lo opuesto; representa a cualquier usuario que acceda al archivo o al directorio mientras trabaja en el servidor. Por ejemplo, si CristinaG accede a un archivo a través de la red (desde su propia estación de trabajo), tendrá los permisos asignados a RED, pero no los que estén asignados a INTERACTIVO. Si utiliza el servidor y accede al mismo archivo desde allí, entonces tendrá los permisos asignados a INTERACTIVO, pero no los de RED.

Los permisos CREADOR PROPIETARIO únicamente pueden asignarse a directorios. Estos permiten representar a los usuarios que posteriormente creen archivos y directorios en el directorio actual. Si concede estos permisos a un directorio, cualquier persona que cree en él un archivo o un subdirectorio recibirá de forma automática los permisos que haya concedido a CREADOR PROPIETARIO para ese archivo o subdirectorio.

Estrategias para el uso de permisos de archivos en NTFS

Se recomienda conceder permisos únicamente a grupos y no a usuarios individuales. Si así lo hace, el servidor será más fácil de mantener. Si hay varios usuarios que necesitan acceder a un conjunto de archivos determinado, puede incorporarlos a un grupo y conceder los permisos necesarios al mismo. Si otro usuario necesita el mismo tipo de acceso, simplemente agréguelo al mismo grupo, en lugar de concederle acceso a cada archivo por separado.

De forma similar, puede ser más conveniente crear grupos locales y asignarles permisos que asignar permisos directamente a grupos globales. Por ejemplo, si existen archivos que deben ver los administradores de todos los grupos de su empresa, deberá crear un grupo local "Todos los administradores" en su dominio y asignarle permisos. De esta manera, si hay más archivos disponibles para los administradores, únicamente tendrá que conceder permiso de acceso al grupo "Todos los administradores" y evitará tener que conceder permisos a todos los grupos globales que contenga "Todos los administradores".

Para obtener más información acerca de las estrategias para el uso de grupos y usuarios, consulte el capítulo 3, "Funcionamiento de la seguridad en la red".

Cuando cree y comparta un archivo o un directorio de un servidor, conceda el permiso Control total al grupo local Administradores. De esta forma, todos los administradores de ese dominio podrán cambiar los permisos y en general, administrar los del archivo o del directorio en el futuro.

Permisos de directorio predeterminado

Cuando se crea un subdirectorio o un archivo en un volumen NTFS, se pueden establecer sus permisos. De lo contrario, el nuevo subdirectorio o archivo heredará los permisos del directorio contenidos en él. Las siguientes tablas muestran los permisos establecidos de forma predeterminada en directorios en Windows NT Advanced Server y Windows NT.

Permisos de directorio predeterminado en Windows NT Advanced Server

● El permiso autoriza el uso
○ El permiso no autoriza el uso

	Control total	Cambio	LSUE	Lectura	LSU	Listado	Sin acceso
\ (Directorios raíz de todos los volúmenes NTFS)							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	○	●	○	○	○	○	○
Todos	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	○	●	○	○	○	○	○
Todos	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\CONFIG							
Administradores	●	○	○	○	○	○	○
Todos	○	○	○	○	○	●	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\DRIVERS							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\SPOOL							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	●	○	○	○	○	○	○
Operadores de impresión	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\REPL							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○

Permisos de directorio predeterminado en Windows NT Advanced Server (cont.)

● El permiso autoriza el uso
○ El permiso no autoriza el uso

	Control total	Cambio	LSUE	Lectura	LSU	Listado	Sin acceso
\SYSTEM32\REPL\IMPORT							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	○	●	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Duplicadores	○	●	○	○	○	○	○
RED	○	○	○	○	○	○	●[1]
\SYSTEM32\REPL\EXPORT							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Duplicadores	○	○	○	●	○	○	○
\USERS							
Administradores	○	○	●	○	○	○	○
Operadores de cuentas	○	○	●	○	○	○	○
Todos	○	○	○	○	○	●	○
\USERS\DEFAULT							
Todos	○	○	○	○	●	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\WIN32APP							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	●	○	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
\TEMP							
Administradores	●	○	○	○	○	○	○
Operadores de servidores	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Todos	○	●	○	○	○	○	○

[1] Debido al método especial con que se conceden los permisos iniciales para el directorio \SYSTEM32\REPL\IMPORT, el permiso "Sin Acceso" asignado a RED no se aplica a los permisos inicialmente otorgados a los grupos Administradores, Operadores de servidores y Todos. Por ejemplo, los Administradores todavía pueden acceder a este directorio a través de la red, ya que en este caso especial su permiso anula el "Sin acceso" asignado a RED.

Permisos de directorio predeterminado en las estaciones de trabajoWindows NT

● El permiso autoriza el uso
○ El permiso no autoriza el uso

	Control total	Cambio	LSUE	Lectura	LSU	Listado	Sin acceso
\ (Directorios raíz de todos los volúmenes NTFS)							
Administradores	●	○	○	○	○	○	○
Todos	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32							
Administradores	●	○	○	○	○	○	○
Todos	○	●	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\CONFIG							
Administradores	●	○	○	○	○	○	○
Todos	○	○	○	○	○	●	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\DRIVERS							
Administradores	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\SPOOL							
Administradores	●	○	○	○	○	○	○
Usuarios avanzados	○	●	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\SYSTEM32\REPL							
Administradores	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○

Permisos de directorio predeterminado en las estaciones de trabajoWindows NT (cont.)

● El permiso autoriza el uso
○ El permiso no autoriza el uso

	Control total	Cambio	LSU/E	Lectura	LSU	Listado	Sin acceso
\SYSTEM32\REPL\IMPORT							
Administradores	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Duplicadores	○	●	○	○	○	○	○
RED	○	○	○	○	○	○	●[1]
\USERS							
Administradores	○	○	●	○	○	○	○
Todos	○	○	○	○	○	●	○
\USERS\DEFAULT							
Todos	○	○	○	○	●	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
\WIN32APP							
Administradores	●	○	○	○	○	○	○
CREADOR PROPIETARIO	●	○	○	○	○	○	○
Todos	○	○	○	●	○	○	○
\TEMP							
Administradores	○	○	●	○	○	○	○
CREADOR PROPIETARIO	○	○	●	○	○	○	○
Todos	○	○	○	●	○	○	○

[1] Debido al método especial con que se concenden los permisos iniciales para el directorio \SYSTEM32\REPL\IMPORT, el permiso "Sin Acceso" asignado a RED no se aplica a los permusos inicialmente otorgados a los grupos Administradores, Operadores de servidores y Todos. Por ejemplo, los Administradores todavía pueden acceder a este directorio a través de la red, ya que en este caso especial su permiso anula el "Sin acceso" asignado a RED.

Además de estos permisos, la identidad especial SISTEMA que representa al sistema operativo tiene permiso Control total para todos los directorios.

Precaución No se debe revocar ninguno de los permisos predeterminados en estos directorios. De lo contrario, algunas partes del sistema operativo no funcionarán. Más aún, no debe utilizar el Administrador de archivos para examinar los permisos en el directorio SYSTEM32\DUPL\IMPORT; si lo hace, se perderán las configuraciones de los permisos especiales de inicio. Estos permisos le permiten al directorio duplicador funcionar sin necesidad de que se los cambie. Para obtener más información acerca del directorio replicador, consulte "Duplicación de directorios" más adelante en este capítulo.

Funcionamiento de los permisos en los volúmenes FAT y HPFS

En los volúmenes FAT y HPFS no es posible asignar permisos individuales a archivos y directorios. El único caso en el que podrá restringir el acceso a un directorio FAT o HPFS es al establecer permisos de recursos compartidos cuando lo comparta, y las restricciones solamente serán aplicables a los usuarios que accedan a él a través de la red.

Cuando comparta un directorio podrá asignar a cada grupo y a cada usuario uno de los cuatro permisos compartidos siguientes: Control total de archivos/directorios, Cambio de archivos/directorios, Lectura de archivos/directorios o Sin acceso a archivos/directorios.

Por ejemplo, si comparte un directorio que deberá contener información sobre los planes del grupo Ingeniería para el año próximo, podría conceder al grupo Administradores de ingeniería el permiso Control total para el directorio compartido, el permiso Lectura al grupo Ingenieros y no conceder ningún permiso a los demás usuarios de la red.

No hace falta asignar el permiso Sin acceso a todos los usuarios que desee excluir del directorio compartido. Simplemente, no conceda al usuario (o a cualquier grupo del que sea miembro el usuario) ningún permiso para el directorio compartido.

El permiso Sin acceso puede serle útil si desea negar a determinados usuarios o grupos el acceso a un directorio, en un caso en que éstos pudieran acceder a él gracias a otros permisos que se les haya asignado. Por ejemplo, podría permitir que todos los usuarios de la red, menos los del grupo Contables, accedan a un directorio compartido si asigna a Todos el permiso Control total y a Contables, Sin acceso.

Uso de auditoría para realizar un seguimiento de los usuarios

Si audita los archivos y directorios de un servidor podrá hacer un seguimiento de su utilización. Podrá identificar quién realizó determinados tipos de acciones con los archivos y directorios, y determinar responsabilidades.

Cuando audite un archivo o un directorio, se escribirá una entrada en el registro de seguridad de Windows NT siempre que se acceda a ellos de una manera determinada. Podrá especificar qué archivos y directorios se auditarán, quién realiza las acciones que desee auditar y exactamente los tipos de acciones que se auditarán.

Para los directorios, podría auditar los intentos logrados y fallidos de realizar los tipos de acceso siguientes:

Tipos de acceso a directorios	Tipos de acceso a archivos
Mostrar los nombres de archivos del directorio	Mostrar los datos del archivo
Mostrar los atributos del directorio	Mostrar los atributos del archivo
Cambiar los atributos del directorio	Mostrar los permisos y el propietario del archivo
Crear subdirectorios y archivos	Cambiar el archivo
Ir a los subdirectorios del directorio	Cambiar los atributos del archivo
Mostrar los permisos y los propietarios de los permisos	Ejecutar el archivo
Eliminar el directorio	Eliminar el archivo
Cambiar los permisos del directorio	Cambiar los permisos del archivo
Cambiar la posesión del directorio	Cambiar la posesión del archivo

Para establecer la auditoría de un archivo o de un directorio, utilice el Administrador de archivos. Para ver las entradas de auditoría, utilice el Visor de sucesos.

Toma de posesión de archivos

Todos los archivos y directorios de un volumen NTFS tienen un *propietario*. El propietario controla los permisos asignados al archivo o directorio, y puede conceder permisos a otros usuarios. La toma de posesión de los archivos es una forma de permitir a los usuarios conservar archivos privados en el servidor (incluso ante los administradores).

Cuando se crea un archivo o un directorio, la persona que los crea se convierte automáticamente en su propietario. Se supone que la mayoría de los archivos de los servidores de red serán creados por los administradores; por ejemplo, cuando instalan aplicaciones en el servidor. Por lo tanto, la mayoría de los archivos de un servidor serán propiedad de los administradores, a excepción de los archivos de datos que creen los usuarios y de los que contengan los directorios particulares de los usuarios.

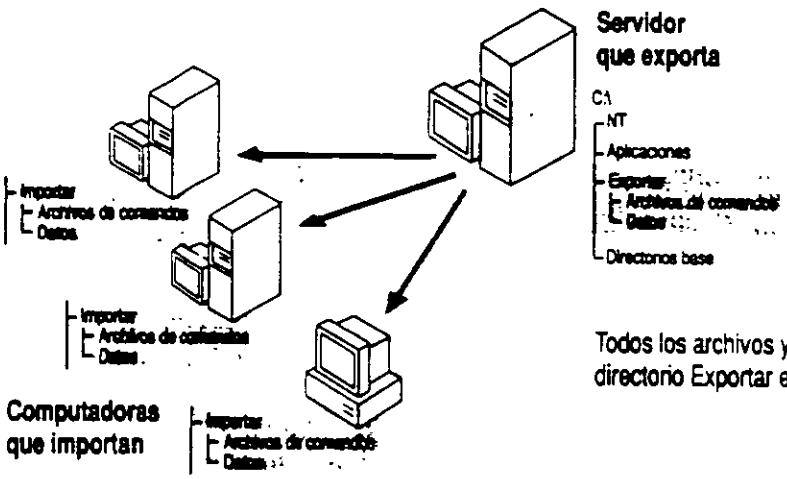
La posesión puede transferirse de dos maneras:

- El propietario actual puede conceder el permiso Tomar posesión a otros usuarios, en cuyo caso dichos usuarios podrán ser propietarios en cualquier momento.
- Un administrador puede tomar la posesión de cualquier archivo en la computadora (ordenador). Por ejemplo, esto podría ser útil si un empleado abandona la empresa repentinamente y el administrador necesita hacerse cargo de los archivos de dicho usuario.

Aunque un administrador puede tomar la posesión, no puede transferirla a otros usuarios. De esta forma, si un administrador toma por error la propiedad de los archivos de un usuario, después no puede devolverla al propietario original. Cuando éste descubra que ya no es el propietario de los archivos, podrá comprobar quién es el propietario actual.

Duplicación de directorios

Con el servicio Duplicador de Windows NT Advanced Server puede configurar y mantener árboles de directorios idénticos en varios servidores y estaciones de trabajo. Cuando actualice un archivo en el árbol de directorios de un servidor (el servidor de Exportación), se copiará automáticamente la lista actualizada a todas las demás computadoras (las computadoras importadoras). Unicamente los servidores que estén ejecutando Windows NT Advanced Server podrán ser servidores de Exportación, mientras que las computadoras importadoras podrán ejecutar Windows NT Advanced Server o Windows NT.



Mediante la provisión de copias idénticas de archivos o aplicaciones a varias computadoras, podrá repartir parte de la utilización de recursos para compartir archivos entre varias computadoras. Si son muchos los usuarios que deben acceder periódicamente a un archivo, puede evitar que un servidor sea desbordado si duplica el archivo en varias computadoras en lugar de proporcionar un único recurso. Después puede permitir que accedan varios usuarios al archivo desde distintas computadoras.

Si lo desea, puede duplicar directorios en las computadoras de otros dominios.

La duplicación de archivos es esencial si utiliza archivos de comandos de inicio de sesión en un dominio que tenga más de un Windows NT Advanced Server.

En las secciones siguientes podrá encontrar más información general acerca de la duplicación de directorios. Si desea instrucciones más detalladas acerca de la duplicación, consulte el capítulo "Administrador de servidores" del *Manual de sistema de Windows NT Advanced Server.*

Funcionamiento de la duplicación de directorios

Para utilizar la duplicación de directorios, primero deberá crear una cuenta de usuario especial que iniciará y controlará internamente el proceso de duplicación.

Después deberá situar los directorios que desea duplicar en el directorio de exportación del servidor de Exportación. Todos los subdirectorios que estén directamente debajo del directorio de exportación podrán ser duplicados en otras computadoras (ordenadores). Para cada uno de dichos directorios, también podrá elegir si desea que se dupliquen sus subdirectorios.

También puede elegir si el servidor de Exportación debe transmitir los cambios en el momento en que se modifique un archivo, o esperar a que se estabilice durante dos minutos el árbol de directorios completo antes de exportar, e impedir así que se exporten árboles con cambios parciales.

Además, puede bloquear un subdirectorio específico del directorio de exportación cuando lo necesite. Los cambios que se efectúen en el directorio bloqueado no se exportarán hasta que lo desbloquee.

En el servidor de Exportación también puede seleccionar qué computadoras o dominios recibirán las copias duplicadas de los directorios que esté exportando dicho servidor.

En cada una de las computadoras importadoras, sencillamente tiene que elegir cuáles son los servidores de los que se duplicarán directorios.

Si lo desea, puede configurar un servidor, de modo que se duplique en él uno de sus propios árboles de directorios (desde su directorio de exportación a su directorio de importación). Con ello puede realizar una copia de seguridad local de los archivos o puede utilizar la versión importada de éstos como otra fuente a la que pueden acceder los usuarios, y conservar la versión de exportación como copia maestra.

Duplicación de archivos de comandos de inicio de sesión

Si utiliza archivos de comandos de inicio de sesión en un dominio que tenga más de un Windows NT Advanced Server, deberá duplicar dichos archivos en los distintos servidores de dominio. Todos los servidores de un dominio autorizan las solicitudes de inicio de sesión. El archivo de comandos de inicio de sesión de un usuario debe estar situado en el servidor que autorice su solicitud de inicio. Al duplicar dichos archivos en todos los servidores está garantizando que siempre estén disponibles para los usuarios, aunque sólo necesitará mantener una copia de cada archivo de comandos.

Para facilitar la duplicación de archivos de comandos de inicio de sesión, Windows NT Advanced Server crea un subdirectorio llamado SCRIPTS dentro de los directorios de importación y de exportación, y lo utiliza para la duplicación. Si decide duplicar los archivos de comandos, deberá utilizar el Administrador de servidores para cambiar la ruta de acceso de cada archivo de comandos del servidor a WINNT\SYSTEM32\DUPL\IMPORT\SCRIPTS o a WINNT\SYSTEM32\DUPL\EXPORT\SCRIPTS, según corresponda. Para obtener más información, consulte el capítulo "Administrador de servidores" del *Manual de sistema de Windows NT Advanced Server*.

El servidor de Exportación de los archivos de comandos de inicio de sesión puede ser el controlador del dominio, aunque no necesariamente.

Ejemplos de archivos compartidos

Configuración de permisos de archivos

Supongamos que necesita establecer permisos para los archivos de un servidor que utiliza un departamento pequeño. El servidor de archivos contiene un directorio de aplicaciones, directorios particulares para cada uno de los usuarios del departamento, un directorio público en el que los usuarios pueden compartir archivos y un directorio buzón, donde éstos pueden archivar informes confidenciales que únicamente puede leer el administrador de grupo.

En el directorio de aplicaciones, convierta todos los programas en archivos de sólo lectura, para impedir la introducción de virus y caballos de Troya. También puede conceder los permisos individuales Cambio de permisos (M) a los administradores, para que un administrador pueda concederse a sí mismo el permiso Escritura cuando deba actualizar una aplicación. Si inicialmente da a los administradores el permiso Escritura, la protección contra virus será menor que si les concede el permiso Cambio de permisos y les obliga a cambiar el permiso antes de actualizar aplicaciones.

Si ninguna de las aplicaciones necesita escribir archivos (por ejemplo, archivos de configuración de inicialización) en sus propios directorios, también deberá **convertir en sólo lectura** los directorios que contengan las aplicaciones.

Para los directorios particulares, conceda a cada usuario el permiso Control total sobre su directorio y no conceda a nadie permisos para ningún otro directorio.

Para el directorio público, puede conceder a todos los usuarios el permiso Cambio, que les permite leer y escribir en este directorio. Este permiso es más apropiado que Control total, puesto que este último les permitiría definir permisos para el directorio público y tomar posesión de él.

Para crear un directorio buzón simplemente conceda al directorio el permiso Lectura y Adición a Usuarios o Todos, y dé el permiso Cambio al administrador que deba leer los archivos del directorio.

No conceda a nadie que no sea un administrador o un operador de servidor el acceso a los archivos, o a los subdirectorios del directorio WINNT.

Configuración de la duplicación de varios árboles de directorios

Supongamos que tiene un dominio en el que desea duplicar dos árboles de directorios, uno para los archivos de comandos de inicio de sesión y otro para datos. Los grupos de computadoras (ordenadores) que necesitan importar ambos árboles son diferentes: sólo los cuatro servidores de dominio necesitan los archivos de comandos, mientras que dos de ellos, junto con dos estaciones de trabajo con Windows NT, necesitan importar los datos.

La mejor solución es configurar servidores diferentes como servidores de Exportación de los directorios de archivos de comandos de inicio de sesión y de los árboles de directorios.

Recuerde que un solo servidor de Exportación tiene únicamente una lista de computadoras importadoras en la que efectúa la duplicación. Si configura un único servidor de Exportación para ambos directorios, exportará ambos árboles de directorios a todas las computadoras exportadoras, incluso aunque no todas éstas utilicen los dos árboles de directorios.

Uso compartido de impresoras

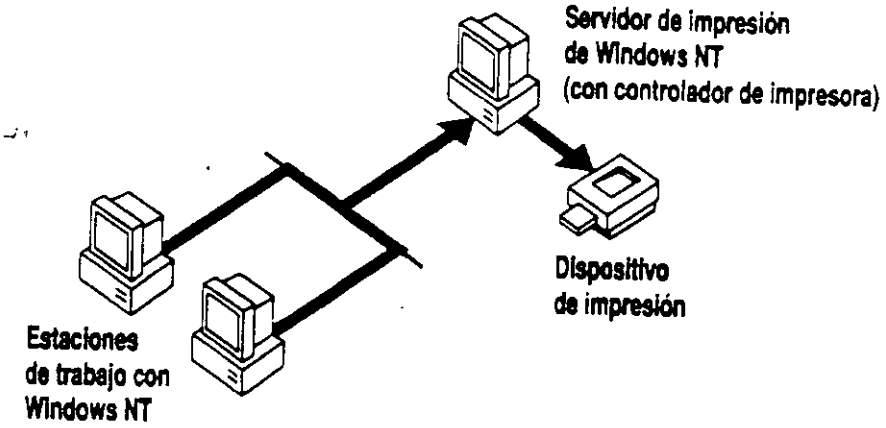
En este capítulo se explican las directrices para configurar y compartir impresoras en una red de Windows NT. Si bien configurar una impresora es una tarea fácil, vale la pena dedicar un poco de tiempo para comprender las diversas opciones de configuración de la impresora. Si planifica cuidadosamente el acceso a las impresoras, podrá aumentar al máximo el rendimiento de cada impresora y, al mismo tiempo, evitar largos tiempos de espera en la cola de impresión.

Descripción general acerca de los procedimientos de impresión en Windows NT

Una red de Windows NT ofrece varias opciones avanzadas de impresión:

- Puede examinar las impresoras de Windows que estén disponibles en la red y después conectarse a una impresora haciendo doble-clic en un nombre de impresora. Encontrará la función "Examinar" en el Administrador de impresión y, aún más convenientemente, en el cuadro de diálogo **Especificar impresora** de las aplicaciones basadas en Windows NT.
- Para utilizar una impresora remota con Windows NT no es necesario instalar los archivos del controlador de impresora en la estación de trabajo local.
- Puede examinar las impresoras de la red que están administradas por otros servidores. Por ejemplo, puede buscar en la red servidores de impresión con LAN Manager 2.x y conectarse a los recursos compartidos de impresión de dichos servidores. En este caso, Windows NT le pedirá que instale localmente el controlador de impresión oportuno si no está ya presente.
- Los servidores de impresión, impresoras, controladores y trabajos de impresión de Windows NT se pueden administrar remotamente.

Cualquier computadora (ordenador) con Windows NT, sea una estación de trabajo o un servidor con Windows NT Advanced Server, puede ejercer de servidor de impresión. Si todos los clientes de impresión utilizan Windows NT, sólo será necesario instalar los archivos de controladores de impresión en el mismo lugar, es decir, en el servidor de impresión.



Planificación de las operaciones de impresión

Puesto que todos los usuarios de la red tendrán que imprimir en alguna ocasión, vale la pena asegurarse de que las operaciones de impresión sean eficientes y económicas. Entre las decisiones que deberá tomar se encuentran:

- Qué impresoras utilizar
- Qué computadoras (ordenadores) utilizar como servidores de impresión
- Cómo configurar las impresoras compartidas para obtener el máximo rendimiento

Selección de impresoras a utilizar

Entre la gama de impresoras modernas se encuentran dispositivos diseñados específicamente para uso en red. Estas impresoras ofrecen opciones como conmutación automática de puertos y emulación, bandejas dobles de alimentación de papel e impresión por las dos caras. Antes de decidir qué impresoras adquirir para su red, evalúe con todo cuidado sus necesidades:

- ¿Necesita pocas impresoras de alto volumen o varias impresoras personales más económicas?

  Las impresoras de alto volumen normalmente tienen más funciones, pero afectan a muchos más usuarios si se averían.

- ¿Cuántas páginas tiene previsto imprimir?

  Probablemente tendrá menos problemas de mantenimiento si el volumen de impresión coincide con el ciclo de trabajo de una impresora (el número de páginas que puede imprimir por mes).

- ¿Qué tipo de gráficos necesita?

  La combinación de las tecnologías Windows NT y TrueType® permite imprimir gráficos y fuentes sofisticados en la mayoría de las impresoras, incluso en aquéllas que normalmente sólo admiten mapas de bits y texto. TrueType está integrado con el entorno de trabajo, por lo cual todas las aplicaciones basadas en Windows NT pueden utilizar fuentes TrueType sin necesidad de modificaciones ni mejoras. Si piensa imprimir muchos gráficos, diagramas o fotografías de medio tono, considere la adquisición de una impresora que admita 300 ppp (puntos por pulgada) o más.

- ¿Qué importancia tiene la rapidez de impresión?

  Mientras que las impresoras tradicionalmente se conectaban a la red a través de los puertos serie o paralelo de las computadoras (ordenadores), las impresoras más modernas se conectan directamente a la red mediante tarjetas LAN incorporadas. Los enlaces de red ofrecen un rendimiento más alto que el disponible actualmente mediante buses paralelo y serie. Sin embargo, los índices de producción de impresión también dependen del tipo de impresora que utilice.

Windows NT admite la mayoría de las impresoras tradicionales, incluyendo impresoras de matriz de puntos, chorro de tinta y láser. También admite impresoras de interfaz de red Hewlett-Packard, como la HP LaserJet IIIsi.

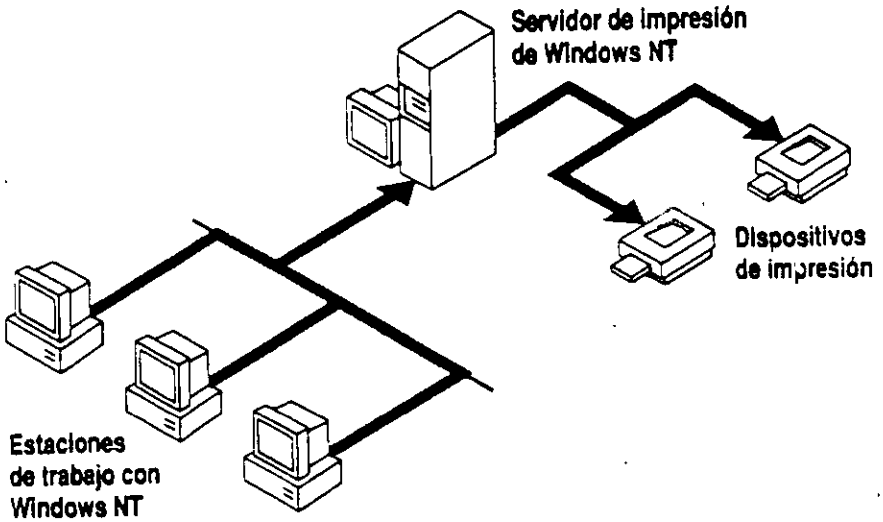
Selección de las computadoras (ordenadores) que vayan a ser servidores de impresión

Sea cual fuere el tamaño de una red, las impresoras probablemente estarán concentradas alrededor de algunas computadoras específicas. Una computadora que actúe como servidor de impresión puede actuar a la vez como servidor de archivos o como estación de trabajo. No existe ningún requisito especial de hardware para los servidores de impresión, excepto que deben tener los puertos de salida adecuados, si utiliza impresoras paralelo o serie.

Para los servidores de impresión basados en microprocesadores x86, serán suficientes 12 MB de RAM para controlar un pequeño número de dispositivos de impresión. Administrar un número elevado de impresoras requiere más memoria. Los requisitos de espacio en disco son mínimos, excepto en aquellos casos en que sea probable que se acumulen los trabajos de impresión.

Combinación de servicios de archivo e impresión

Cuando utilice Windows NT Advanced Server para compartir archivos e impresión, las operaciones con archivos tienen la primera prioridad (las operaciones de impresión nunca demoran el acceso a los archivos). De manera similar, las operaciones con archivos tienen repercusiones mínimas sobre las impresoras conectadas directamente al servidor; los puertos paralelo y serie son siempre el cuello de botella más importante. Un servidor de impresión dedicado será necesario solamente en los casos en que éste deba administrar muchas impresoras de tráfico intenso.



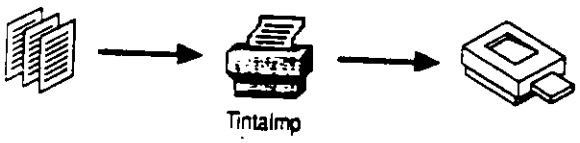
La decisión de combinar servidores de impresión y de archivos puede depender de sus criterios de seguridad. Mientras que las impresoras siempre deben estar disponibles para las personas que las utilicen, podría ser conveniente bloquear un servidor de archivos.

Planificación del acceso de los usuarios a las impresoras

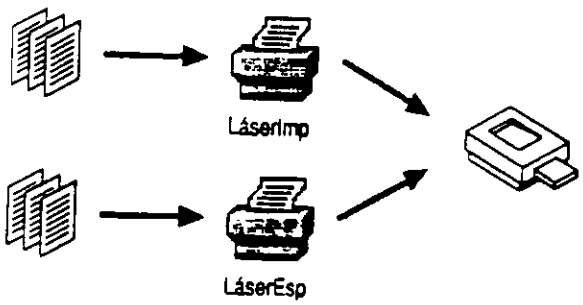
Antes de instalar impresoras en un servidor, debe conocer las opciones de configuración que pueden mejorar la flexibilidad y la eficacia de la impresión en una red. Tras estudiar estas opciones, estará preparado para utilizar el Administrador de impresión para instalar y configurar las impresoras.

Para aprovechar las ventajas de las diversas configuraciones de impresión, primero deberá entender la diferencia entre un *dispositivo de impresión*, que se conecta a una computadora (ordenador) o a la red, y una *impresora lógica*, que se puede crear utilizando el Administrador de impresión de Windows NT. Un *dispositivo de impresión* es un elemento de hardware mecánico que realmente imprime, como una impresora Hewlett-Packard LaserJet. La impresora que cree utilizando el Administrador de impresión será una interfaz de software entre el sistema operativo y el dispositivo de impresión, que define a qué lugar irá el documento antes de llegar al dispositivo de impresión (a un puerto local, a un archivo o a un recurso compartido de impresión remoto), cuándo debe ir y otros aspectos del proceso de impresión. Cuando los usuarios se conecten con las impresoras, se estarán conectando con nombres de impresora lógicos que representan a uno o más dispositivos de impresión.

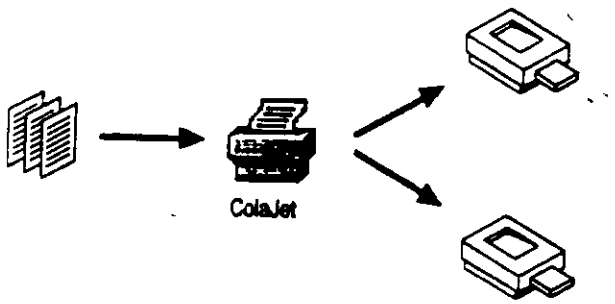
Asociando de distintas maneras las impresoras lógicas y los dispositivos de impresión, podrá ofrecer a los usuarios flexibilidad para sus operaciones de impresión. Son posibles diversas configuraciones, como se muestra en los diagramas a continuación.



De impresora individual a dispositivo de impresión individual



De múltiples impresoras a dispositivo de impresión individual



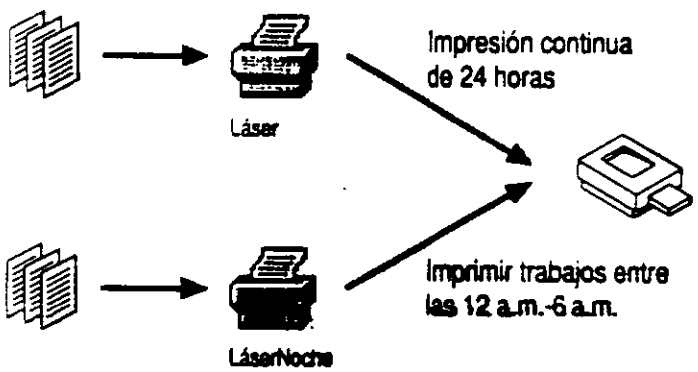
De impresora individual a múltiples dispositivos de impresión

La capacidad de asignar más de una impresora lógica a un dispositivo de impresión ofrece a los usuarios flexibilidad para imprimir documentos. Por ejemplo, dos impresoras lógicas asociadas a un solo dispositivo de impresión pueden ofrecer distintas propiedades de impresión: una puede imprimir un separador de páginas y la otra no. Una impresora lógica podría acumular trabajos e imprimirlos por la noche, mientras que la otra procesaría los trabajos 24 horas al día.

En el resto de esta sección se explica cómo pueden mejorarse la flexibilidad y la eficacia de la impresión mediante distintas configuraciones.

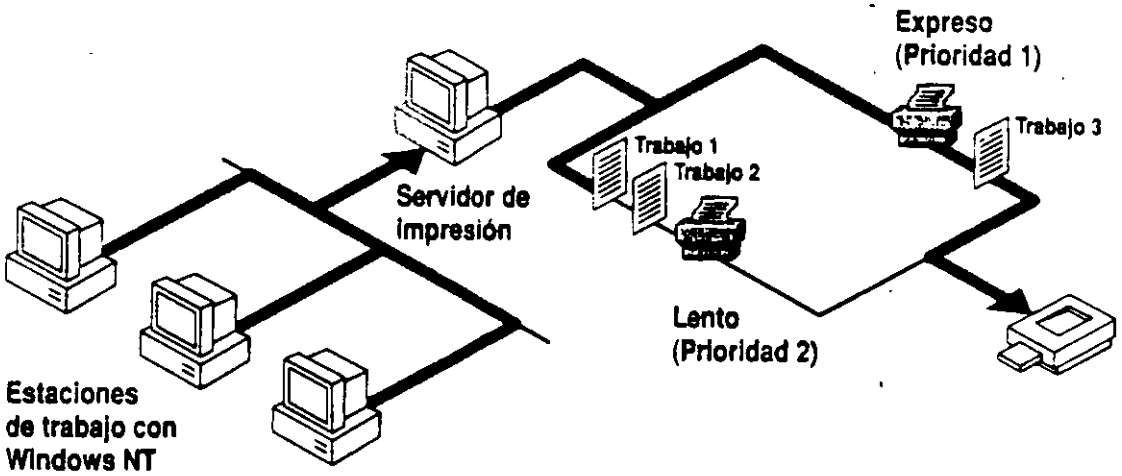
Suspensión de trabajos de impresión

Una buena manera de aumentar al máximo el rendimiento de los dispositivos de impresión es escalonar los tiempos de impresión. Para ello, utilice el Administrador de impresión para definir las horas durante las cuales una impresora puede imprimir trabajos. Si especifica horas de impresión, el administrador de colas de impresión aceptará los trabajos en cualquier momento, pero no los imprimirá en el dispositivo de impresión correspondiente hasta la hora de comienzo programada. A la hora de detener la impresión, el administrador de colas dejará de enviar trabajos al dispositivo de impresión y guardará los trabajos restantes hasta la hora de comienzo de impresión. Si el tráfico de la impresora es intenso durante el día, puede postergar la impresión de los trabajos menos importantes, encaminándolos a través de una impresora que únicamente imprima en horas libres.



Concesión de niveles de prioridad para impresoras

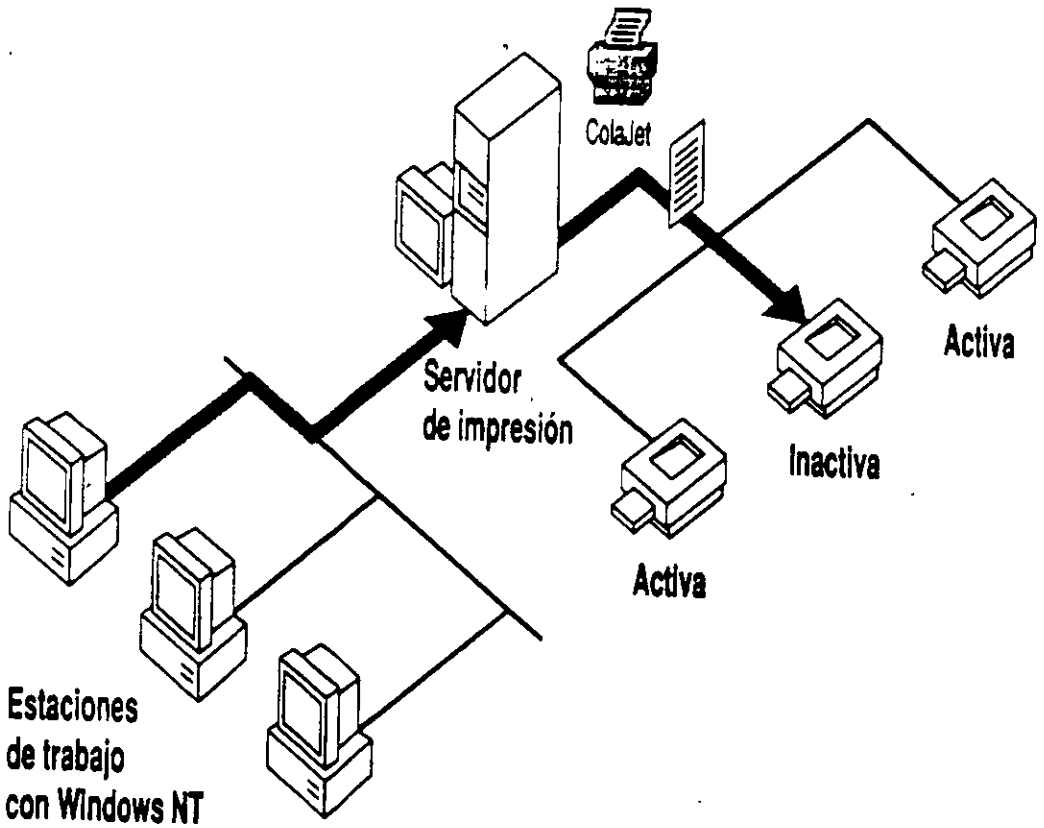
En algunas ocasiones es posible que necesite imprimir un documento inmediatamente y desee saltar los trabajos que estén en espera en un dispositivo de impresión determinado. Esto puede hacerlo si crea impresoras con diferentes niveles de prioridad (la prioridad de impresión se establece en el cuadro de diálogo **Detalles** del Administrador de impresión). Si dos impresoras lógicas tienen asignado un único dispositivo de impresión, los trabajos se encaminan a la impresora cuyo nivel de prioridad sea más alto (número más bajo).



Para aprovechar al máximo este sistema de prioridades de impresión, cree varias impresoras conectadas a un mismo dispositivo de impresión. Asigne a cada impresora un nivel de prioridad y después cree un grupo de usuarios para cada impresora. Por ejemplo, los usuarios del Grupo 1 podrían tener derechos de acceso a una impresora de prioridad 1, los usuarios del Grupo 2 podrían tener derechos de acceso a una impresora de prioridad 2, etc. De esta forma, podrá definir las prioridades de los trabajos de impresión según el tipo de usuario.

Uso de un grupo de impresoras

Un grupo de impresoras consiste de dos o más dispositivos de impresión similares asociados a una sola impresora lógica. Para configurar un grupo, debe crear una impresora lógica utilizando el Administrador de impresión y asignarle tantos puertos de salida como dispositivos de impresión idénticos tenga (Windows NT no tiene límite para el número de impresoras de un grupo). El siguiente trabajo de impresión será recibido por el dispositivo de impresión que esté libre. Esta configuración aprovecha al máximo el uso de los dispositivos de impresión, a la vez que reduce al mínimo la cantidad de tiempo que deben esperar los usuarios para imprimir sus trabajos.



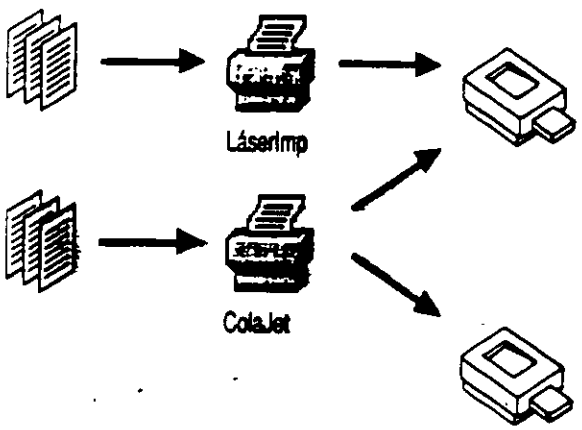
Los grupos de impresoras tienen las siguientes características:

- Todos los dispositivos del grupo comparten el mismo modelo de impresión y actúan como una sola unidad. Las propiedades de impresión se aplican al grupo completo.
- Los puertos de impresora pueden ser del mismo tipo o pueden ser distintos (serie, paralelo y red).

- Cuando un trabajo llega al grupo de impresoras, el administrador de colas comprueba los destinos de salida de la impresora, para ver qué dispositivo está libre. El primer puerto instalado es el primero que se comprueba, después el segundo, etc. Si el grupo consta de distintos tipos de puertos, asegúrese de seleccionar primero el puerto más rápido (red, después paralelo y después serie).
- Si un dispositivo de un grupo deja de imprimir (cuando se quede sin papel, por ejemplo) se mantendrá en espera un solo trabajo de impresión en ese dispositivo. Los demás trabajos continuarán imprimiéndose en otros dispositivos del grupo mientras el trabajo detenido aguarda a que se repare el dispositivo que haya dejado de funcionar.

Es imposible predecir qué impresora de un grupo recibirá un trabajo en particular. No obstante, si está activo el servicio de Mensajería de Windows NT, una estación de trabajo obtendrá mensajes indicándole cuándo terminan los trabajos de impresión e identificará la impresora por el puerto de salida. Salvo que desee que los usuarios dependan de estos mensajes, será conveniente situar las impresoras del grupo en un mismo lugar.

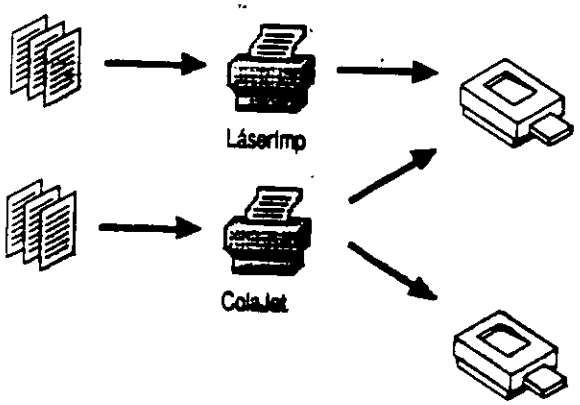
Una configuración de impresoras particularmente eficaz es aquélla en la que puede accederse a un dispositivo de impresión desde dentro y desde fuera de un grupo de impresión, como se muestra a continuación. Esta configuración ofrece el excelente rendimiento de un grupo de impresión y la flexibilidad de disponer de más de una impresora lógica.



- Cuando un trabajo llega al grupo de impresoras, el administrador de colas comprueba los destinos de salida de la impresora, para ver qué dispositivo está libre. El primer puerto instalado es el primero que se comprueba, después el segundo, etc. Si el grupo consta de distintos tipos de puertos, asegúrese de seleccionar primero el puerto más rápido (red, después paralelo y después serie).
- Si un dispositivo de un grupo deja de imprimir (cuando se quede sin papel, por ejemplo) se mantendrá en espera un solo trabajo de impresión en ese dispositivo. Los demás trabajos continuarán imprimiéndose en otros dispositivos del grupo mientras el trabajo detenido aguarda a que se repare el dispositivo que haya dejado de funcionar.

Es imposible predecir qué impresora de un grupo recibirá un trabajo en particular. No obstante, si está activo el servicio de Mensajería de Windows NT, una estación de trabajo obtendrá mensajes indicándole cuándo terminan los trabajos de impresión e identificará la impresora por el puerto de salida. Salvo que desee que los usuarios dependan de estos mensajes, será conveniente situar las impresoras del grupo en un mismo lugar.

Una configuración de impresoras particularmente eficaz es aquélla en la que puede accederse a un dispositivo de impresión desde dentro y desde fuera de un grupo de impresión, como se muestra a continuación. Esta configuración ofrece el excelente rendimiento de un grupo de impresión y la flexibilidad de disponer de más de una impresora lógica.



Conexión de impresoras a la red

Tras decidir cómo desea que los usuarios compartan las impresoras de la red, estará preparado para conectar los dispositivos de impresión a la red. Las impresoras compartidas pueden conectarse a los puertos serie o paralelo de una computadora (ordenador), o directamente a la red, si disponen de una tarjeta adaptadora de red incorporada.

Configuración de impresoras en paralelo y en serie

Las impresoras se conectan a las computadoras (ordenadores) a través de puertos paralelo o serie. Las impresoras conectadas mediante cables paralelo deben estar situadas a una distancia inferior a los 6 metros del servidor; los cables serie pueden tener una longitud de hasta 30 metros. Las computadoras estándar compatibles con IBM admiten tres puertos paralelo y dos puertos serie. Las computadoras tipo RISC generalmente vienen provistas de un puerto paralelo y dos puertos serie incorporados, y admiten tantos puertos adicionales como espacio tengan para ellos.

La configuración de puertos paralelo puede requerir el ajuste de puentes o interruptores de hardware. Las comunicaciones tipo serie requieren protocolos, que establecen un método para que la impresora indique a Windows NT que el búfer está lleno. Los puertos serie pueden configurarse como Sin protocolo, XON/XOFF, Protocolo de software o Protocolo de hardware, si elige el icono Puertos en el Panel de control de Windows NT. En la documentación de la impresora podrá encontrar la configuración de comunicaciones que deberá utilizar. Normalmente, la configuración es de 9600 baudios, sin paridad, 8 bits, 1 bit de paro y Protocolo de hardware.

Si utiliza una impresora serie, use el cable que se suministró originalmente con el dispositivo. Los diagramas de conexiones a menudo varían con los distintos cables.

Definición de los niveles de interrupción del hardware

El número de impresoras y otros dispositivos que pueden conectarse a una computadora (ordenador) depende del número de ranuras de tarjeta de interfaz, direcciones y líneas de solicitud de interrupción (IRQ) disponibles. Por ejemplo, aunque Windows NT admite un número ilimitado de puertos serie y paralelo, encontrar un nivel de IRQ disponible podría ser difícil, puesto que las computadoras con un bus AT® pueden tener un número limitado de IRQs. Los dispositivos estándar COM1, COM2, LPT1 y LPT2 están asignados a los siguientes IRQs:

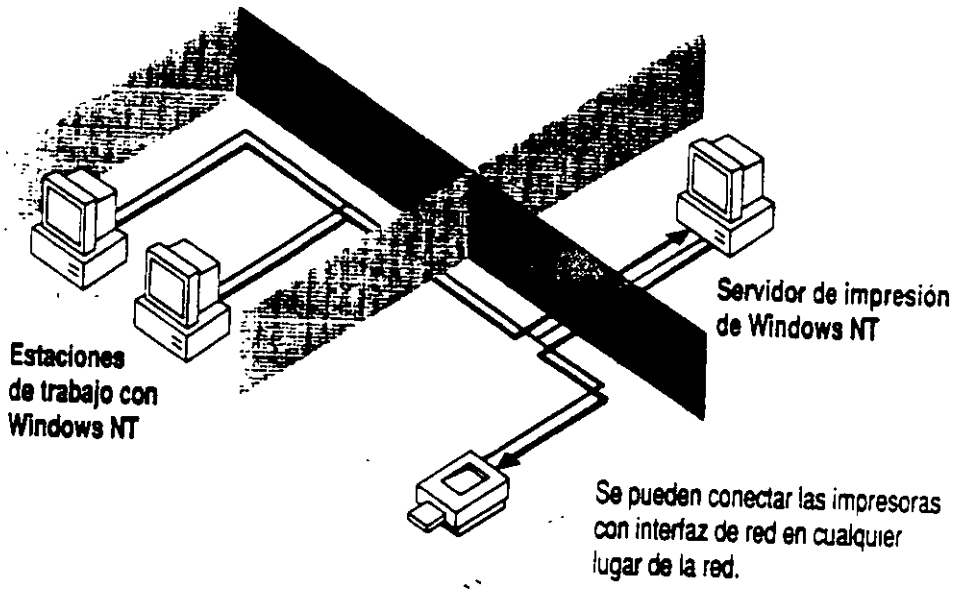
```
COM1 = IRQ4
COM2 = IRQ3
LPT1 = IRQ7
LPT2 = IRQ5
```

En las computadoras tipo RISC, LPT1, COM1 y COM2 están incorporados y no producen conflictos con los niveles de IRQ del bus EISA. Esto libera los IRQ 3, 4 y 7 para otros dispositivos.

Algunas tarjetas de interfaz admiten el uso compartido de interruptores. Esto significa que dos direcciones de dispositivo pueden utilizar el mismo nivel de IRQ. Sin embargo, algunos dispositivos pueden requerir del uso exclusivo de determinados interruptores. Para evitar conflictos, lea los manuales de hardware de estos dispositivos antes de configurar los puertos. Para averiguar la configuración actual de IRQ de su computadora, ejecute el programa de diagnóstico de Microsoft (\WINNT\SYSTEM32\MSD32.EXE). Para obtener más información acerca de la configuración de los IRQ, consulte "Solución de problemas" en el *Manual de sistema de Windows NT Advanced Server*.

Configuración de impresoras de la interfaz de red

A diferencia de los dispositivos paralelo y serie, las impresoras que tengan tarjetas adaptadoras de red incorporadas no tienen que estar situadas junto al servidor de impresión. La ubicación de estos tipos de impresoras no tiene repercusiones sobre la ejecución de la impresión, siempre que los usuarios y las impresoras no estén en lados opuestos de un puente de red. Un servidor de impresión con Windows NT puede controlar un número ilimitado de impresoras de interfaz de red de Hewlett-Packard. Para mantener niveles altos de rendimiento del servidor, aumente la memoria cuando agregue impresoras.



Las impresoras de interfaz de red se conectan a la red a través de una tarjeta adaptadora incorporada. Para utilizar una impresora de interfaz de red de HP, por ejemplo, la impresora HP LaserJet IIIsi, tendrá que instalar el protocolo Control de vínculos de datos (suministrado con Windows NT). Esto puede hacerlo durante la ejecución del programa de instalación o, posteriormente, mediante el icono Red del Panel de control.

Tras conectar una impresora de interfaz de red, ejecute una prueba de autocomprobación para obtener la dirección de la tarjeta de red. Cuando instale la impresora en el servidor, elegirá esta dirección de tarjeta de la lista de direcciones de impresoras disponibles. Para obtener instrucciones acerca de cómo configurar una impresora de interfaz de red, consulte el capítulo 6, "Administrador de impresión", en el *Manual de sistema de Windows NT Advanced Server*.

Creación de impresoras en un servidor

Después de conectar físicamente los dispositivos de impresión, necesitará instalarlos en una computadora (ordenador). Para ello, cree impresoras en el servidor de impresión que desee utilizando el Administrador de impresión de Windows NT. Para crear impresoras en computadoras remotas con Windows NT, utilice el comando **Visor de servidores** del Administrador de impresión para centrarse en la computadora en la cual desee crear las impresoras. Para crear una impresora, debe ser miembro de uno de los grupos siguientes: Administradores, Operadores de servidor u Operadores de impresión.

Para crear una impresora debe asignar determinadas características o *propiedades*. Por ejemplo, puede especificar que una impresora únicamente imprima a determinadas horas o que genere un separador de páginas. La manera de configurar las propiedades dependerá del modo en que desee que los usuarios accedan a los dispositivos de impresión (consulte la sección anterior, "Planificación del acceso de los usuarios a las impresoras").

Independientemente de sus planes de configuración de impresoras, cuando cree una impresora debe establecer las siguientes propiedades:

- Nombre de impresora
- Controlador de impresora
- Destino de impresión

Después de definir estas propiedades, se le pedirá que configure propiedades específicas del dispositivo (fuentes, memoria de la impresora, color, etc.). Si no realiza modificaciones en una propiedad específica, Windows NT imprimirá utilizando la configuración predeterminada.

También debe *compartir* la impresora para que puedan acceder a ella los usuarios de la red. Normalmente, la configuración predeterminada del resto de las propiedades de impresión bastará para que se pueda imprimir.

Desde el momento en que empiece a compartir una impresora, ésta aparecerá en la lista de impresoras de la red del Administrador de impresión. Los usuarios podrán elegir las impresoras de Windows NT que aparezcan en esta lista si seleccionan **Conectar a impresora** en el Administrador de impresión. También podrán elegir **Especificar impresora** en el menú **Opciones** de una aplicación de Windows y, después, seleccionar el botón "Red".

Los usuarios también pueden conectarse a las impresoras de Windows NT si crean una impresora local y después redirigen el puerto local mediante el Administrador de impresión. No obstante, esto requiere que esté instalado un controlador de impresora local en la estación de trabajo del usuario.

Instalación de controladores de impresora

Un *controlador de impresora* es un programa que convierte comandos de gráficos en el lenguaje específico de impresión, por ejemplo, PostScript® o PCL®. Los controladores de impresora también contienen información importante que Windows NT necesita saber acerca de la impresora, como detalles acerca de su hardware, incluyendo descripciones de fuentes y tamaños de papel.

Windows NT tiene controladores para la mayoría de los dispositivos de impresión disponibles en el mercado. Cuando seleccione un nombre de controlador de impresora, el Administrador de impresión solicitará la ubicación del controlador (aquí puede indicar un nombre de ruta de acceso o una unidad de disquetes). Para instalar un controlador no suministrado por Windows NT, seleccione "Otro" en la lista "Controlador". Windows NT solicitará el nombre y la ubicación del controlador.

Las computadoras (ordenadores) tipo RISC y tipo x86 requieren controladores de impresora diferentes. Para utilizar una impresora creada en una computadora con Windows NT tipo x86, un cliente con RISC requerirá un controlador de impresora tipo RISC apropiado para esa impresora. El controlador puede estar instalado localmente o en el servidor de tipo x86. De manera similar, los clientes con computadoras tipo x86 únicamente pueden utilizar un servidor de impresión tipo RISC si los controladores tipo x86 requeridos están instalados localmente o en el servidor.

Si la red contiene una combinación de computadoras tipo RISC y tipo x86, podrá instalar ambos tipos de controladores en sus servidores de impresión. Con ello se asegurará de que los trabajos de impresión que se originen en uno u otro tipo de computadora puedan utilizar todos los dispositivos de impresión. Por ejemplo, si el servidor de impresión es una computadora tipo x86, instale el controlador apropiado para su dispositivo de impresión eligiéndolo de la lista de controladores. Después elija "Otro" en dicha lista e instale el controlador para RISC adecuado para el mismo dispositivo. El Administrador de impresión determinará si las solicitudes de impresión entrantes son de tipo RISC o x86, y utilizará el controlador apropiado de forma automática si es que está presente.

Si no se admite un controlador determinado, intente configurar la impresora como se describe en la siguiente tabla:

Si se trata de una	Configúrela como una
Impresora láser:	
Compatible con HPPCL (LaserJet)	Hewlett-Packard LaserJet Plus®.
Compatible con PostScript	QMS®-ColorScript.
PostScript color	Apple® LaserWriter® Plus.
Conjunto o superconjunto de fuentes de 35 fuentes	
Impresora matriz:	
Matriz de 9 agujas	
Compatible con IBM	IBM Proprinter™.
Compatible con Epson®	Epson FX-80 para carro estrecho o FX-100 para carro ancho.
Matriz de 24 agujas	
Compatible con IBM de 24 agujas	IBM Proprinter X24.
Compatible con Epson LQ	Epson LQ-1500.
Otra:	Póngase en contacto con el fabricante para averiguar si dispone de controladores personalizados.

Para obtener información acerca de cómo adquirir nuevos controladores de impresora para el sistema, póngase en contacto con el fabricante del hardware o con los servicios de asistencia a clientes de Microsoft.

Selección de un destino de impresión

Cuando cree una impresora deberá indicar al Administrador de impresión dónde desea que imprima. Una impresora puede imprimir en uno o más de los siguientes tipos de destinos: un puerto de salida local, un archivo, un nombre compartido de impresión remoto o una dirección de impresora de la red. Si configura una impresora de modo que imprima en más de un destino, estará creando un grupo de impresoras.

Los siguientes destinos de impresión aparecen como opciones en el Administrador de impresión:

- LPT1 a LPT3 representan puertos paralelos.
- COM1 a COM4 representan puertos serie. Se pueden configurar más puertos serie si utiliza la opción "Puertos" en el Panel de control.
- ARCHIVO le permite imprimir directamente a un archivo. Esta opción no es recomendable para las impresoras de red, puesto que el mensaje que pregunta el nombre del archivo aparecerá en el servidor y no en la estación de trabajo del usuario.
- La impresora de red ofrece las siguientes selecciones:
  - Puerto local es un puerto que no ha sido instalado previamente.
  - Puerto Hewlett-Packard Network permite al usuario seleccionar una dirección de impresora de red de Hewlett-Packard. Tendrá esta opción sólo si el protocolo DLC ha sido instalado.

Uso de separadores de páginas

Puede configurar una impresora de forma que imprima uno o más separadores de páginas al principio de una tarea de impresión. En el separador de páginas suele imprimirse el nombre del usuario remitente de la tarea, y la fecha y hora de impresión.

Podrá seleccionar un archivo del separador de páginas a través del botón "Detalles" del cuadro de diálogo **Propiedades** del Administrador de impresión. Introduzca el nombre del archivo del separador de páginas o examine los directorios y seleccione un archivo. El archivo puede ser uno de los cuatro separadores de páginas que vienen incluidos con Windows NT o puede ser un separador de páginas personalizado que haya creado.

La siguiente tabla muestra los nombres de los archivos de separadores de páginas que vienen incluidos con Windows NT, la función de cada uno, el tipo de impresora con la cual cada archivo es compatible, y si son o no modificables. De forma predeterminada, los archivos de separadores de páginas se almacenan en el directorio \WINNT\SYSTEM32.

Nombre de archivo	Función	Compatible con	¿Modificable?
DEFAULT.SEP	Imprime una página delante de cada documento	PCL	No
PSLANMAN.SEP	Imprime una página delante de cada documento	PostScript	Sí
PCL.SEP	Cambia la impresora a modo de impresión PCL	PCL	Sí
PSCRIPT.SEP	Cambia la impresora a modo de impresión PostScript	PostScript	Sí

DEFAULT.SEP no es un archivo en el disco sino un archivo integrado dentro del programa. Para utilizarlo, escriba **DEFAULT.SEP** directamente.

Para crear su propio separador de páginas, puede modificar y volver a nombrar uno de los separadores predeterminados. La tabla siguiente describe los códigos de escape que pueden incluirse en un archivo del separador de páginas. Windows NT reemplaza estos códigos por los correspondientes datos para su envío directo a la impresora.

Los códigos de escape siempre comienzan con un carácter de escape y terminan con una letra o número. La primera línea del separador de páginas sólo deberá contener el código de escape. En la siguiente tabla, asuma que la variable @ es el primer carácter (el carácter de escape) en el archivo.

Código de escape	Función
@N	Imprime el nombre del usuario que solicitó la tarea.
@I	Imprime el número del trabajo.
@D	Imprime la fecha de impresión del trabajo. La fecha aparece en el formato que se especificó en el cuadro "Formato de fecha" en el icono Internacional del Panel de control.
@T	Imprime la hora a la cual se imprimió la tarea. La hora aparece en el formato que se especificó en el cuadro "Formato de hora" en el icono Internacional del Panel de control.
@L*xxxx*	Imprime todos los caracteres (*xxxx*) que lo sigan hasta el próximo código de escape.
@Fpathname	Imprime el contenido del archivo especificado por el nombre de ruta (pathname) a partir de la primera línea en blanco. El contenido de este archivo se copia directamente a la impresora sin mediar procesamiento alguno.
@H*nn*	Establece una secuencia de control para una impresora específica, donde *nn* es un código hexadecimal ASCII que se envía directamente a dicha impresora. Encontrará estos números en el manual de su impresora.
@W*nn*	Fija el ancho del separador de páginas. El ancho predeterminado es 80. El ancho máximo es 256. Todo carácter imprimible que sobrepase el ancho máximo aparecerá truncado.
@U	Desactiva la impresión en bloque de caracteres.
@B@S	Imprime texto en bloques de caracteres de ancho único hasta que encuentre el próximo código @U.
@E	Expulsa una página de la impresora. Utilice este código para iniciar un nuevo separador de páginas o para concluir el archivo de separador de páginas. Si al imprimir un trabajo sale un separador de páginas en blanco, suprima este código de su archivo de separador de páginas.
@*n*	Omite *n* número de líneas (del 0 hasta el 9). Omitir 0 líneas sólo desplaza la impresión a la siguiente línea.
@B@M	Imprime texto en bloques de caracteres de ancho doble hasta que encuentra el código @U.

Configuración de propiedades para dispositivos específicos

Las propiedades de dispositivos de impresión específicos describen la configuración física de los mismos (de cuántas plumas de trazador dispone, de cuánta memoria, etc). Estas propiedades son distintas para cada dispositivo.

Cuando cree una impresora, utilice el Administrador de impresión para asegurarse de que las propiedades de un dispositivo específico concuerdan con la configuración del dispositivo de impresión. Aunque la configuración predeterminada satisfaga numerosas necesidades de impresión, muchas opciones especiales, como las disponibles con los controladores de impresora PostScript, requieren una configuración personalizada.

Es fácil confundir la configuración de una impresora específica con las propiedades de un trabajo. La configuración de un trabajo no depende de la configuración física de un dispositivo. Si una aplicación no configura una propiedad de un trabajo, como por ejemplo, la orientación de la página o el tamaño del papel, el dispositivo de impresión toma como valores predeterminados las propiedades de los trabajos definidas en el Administrador de impresión. La configuración de la aplicación siempre tiene precedencia sobre los valores predeterminados para trabajos configurados en el Administrador de impresión. En las siguientes listas se muestran propiedades de trabajos e impresoras específicas.

Propiedades de dispositivos específicos:	**Propiedades de trabajos:**
Color	Número de copias
Resolución	Orientación de página
Memoria	Impresión a dos caras
Nombre del cartucho de fuentes	Intercalar copias
Ubicación del formato	Formato
Pluma de trazador	

Configuración de la memoria de la impresora

Si utiliza una impresora de páginas, como una impresora láser, es importante asegurarse de que la cantidad de memoria disponible en el dispositivo concuerda con el valor mostrado en el cuadro "Memoria de la impresora". Esta configuración de dispositivo específico aparece en el cuadro de diálogo **Configuración de impresora** después de instalar un controlador de dispositivo. Puesto que las impresoras de páginas necesitan almacenar una página completa en la memoria, requieren cantidades de memoria relativamente grandes.

Si la impresora dispone de una memoria mucho mayor o menor de lo que se muestra en el cuadro "Memoria de la impresora", la ejecución de la impresión puede verse afectada. Por ejemplo, Windows NT puede intentar almacenar más fuentes a la impresora de las que ésta pueda manejar razonablemente. Las pruebas de autocomprobación de la impresora suelen indicar cuánta memoria RAM posee el dispositivo.

Uso de formatos

Windows NT mantiene una base de datos de formatos. Un formato consiste en un tamaño físico de papel, márgenes que definen la zona de impresión y un nombre. Los usuarios pueden definir nuevos formatos y agregarlos a la base de datos. De esta forma, podría crear un formato denominado LEGAL5 que use papel de tamaño legal y márgenes de 5 centímetros.

Si un dispositivo de impresión tiene un formato de tamaño legal en la bandeja superior y un formato de tamaño carta en la bandeja inferior, deberá configurar las propiedades de la impresora de acuerdo a estas características. Tenga en cuenta que el controlador de impresora indica automáticamente los tamaños físicos de los formatos que puede aceptar, pero no ofrece la opción de especificar formatos que el controlador de dispositivo no sea capaz de procesar.

Un usuario elige el formato que desee utilizar en un documento específico a través del software de una aplicación. Las aplicaciones basadas en Windows NT permiten a los usuarios imprimir distintas partes de un documento en distintos formatos.

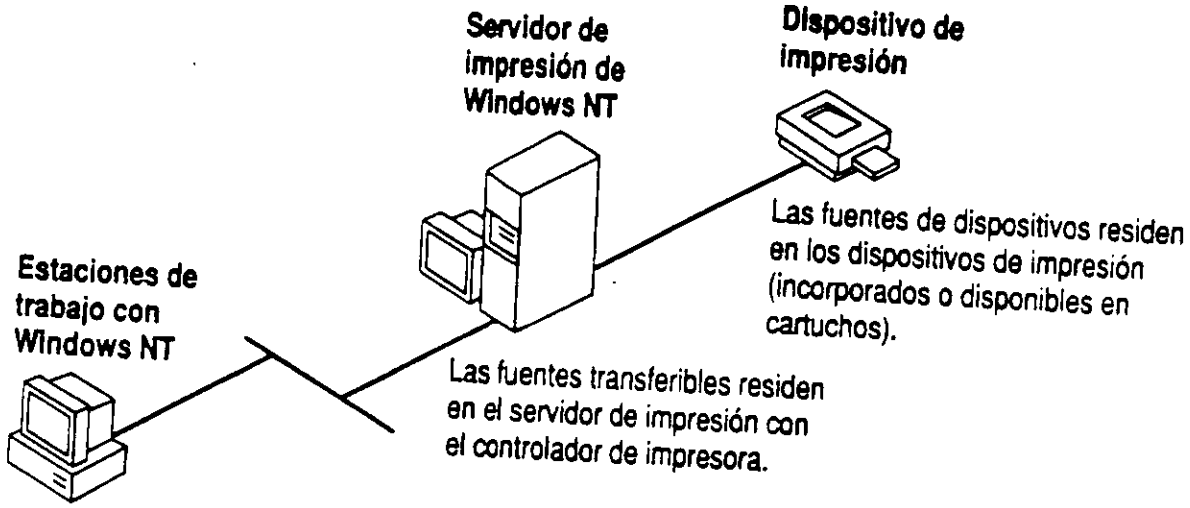
Selección de fuentes

Las fuentes son conjuntos de caracteres y símbolos que tienen un diseño y una resolución específicos. Los dispositivos de impresión utilizan tres tipos de fuentes:

- Las *fuentes de dispositivo* son fuentes que residen realmente en el hardware de la impresora. Pueden estar incorporadas en la propia impresora, en un cartucho o en una tarjeta de fuentes.
- Las *fuentes de pantalla* son fuentes de Windows NT que pueden convertirse para salida impresa. Entre éstas se encuentran las fuentes TrueType. Para instalar fuentes de pantalla, utilice la opción "Fuentes" del Panel de control.
- Las *fuentes transferibles* son fuentes que se instalan en el mismo lugar en el cual esté instalado un controlador de dispositivo. De esta manera, cuando las computadoras (ordenadores) con Windows NT utilicen las impresoras instaladas en un servidor de impresión remoto de Windows NT, las fuentes transferibles solamente deberán estar presentes en el servidor de impresión. Una computadora con MS-DOS que redirije un puerto de salida para utilizar la misma impresora deberá instalar localmente las fuentes transferibles (y el controlador de dispositivo). En las computadoras con Windows NT, utilice el Administrador de impresión para instalar fuentes transferibles.

No todos los dispositivos pueden utilizar los tres tipos de fuentes de impresora mencionados. Por ejemplo, los trazadores de plumas normalmente no pueden utilizar fuentes transferibles ni imprimir fuentes de pantalla de líneas.

Para cada documento, Windows NT transfiere las fuentes transferibles y de pantalla requeridas al dispositivo de impresión. Se puede reducir el tiempo de impresión si se utilizan fuentes de dispositivo, que ya están presentes en la impresora.



Windows NT incluye tres tipos de fuentes de pantalla que pueden reproducirse en la impresora:

- Las *fuentes TrueType* son fuentes independientes de los dispositivos que pueden reproducirse en todos los dispositivos de impresión. Las fuentes TrueType se almacenan como perfiles que pueden escalarse y girarse. Para reproducirlas en un dispositivo de impresión, sólo es necesario que estén presentes en la computadora (ordenador) que origine un trabajo de impresión.
- Las *fuentes de líneas* se almacenan como mapas de bits y dependen del dispositivo. Si una impresora no es compatible con la fuente, no podrá imprimirla. Las fuentes de líneas no pueden girarse ni escalarse.
- Las *fuentes vectoriales* son útiles para dispositivos como trazadores, que no pueden reproducir mapas de bits. Su escala puede ajustarse a cualquier relación de tamaño o aspecto.

La mayor ventaja de las fuentes TrueType en un entorno de red es su portabilidad. Los documentos con fuentes TrueType son independientes del dispositivo de impresión, de la aplicación o del sistema.

Uso compartido de impresoras en red

Para compartir impresoras con otras estaciones de trabajo, debe marcar una casilla de verificación en el Administrador de impresión. Esto asigna automáticamente un *nombre de recurso compartido* a su impresora. Este nombre de recurso compartido lo utilizan las estaciones de trabajo que no reconozcan los nombres de impresora (y de archivos) largos que utiliza Windows NT. Las computadoras (ordenadores) con Windows NT no utilizan nombres de recurso compartido para identificar a las impresoras. En su lugar utilizan nombres de impresora (que pueden tener hasta 32 caracteres).

Si comparte impresoras con estaciones de trabajo con MS-DOS, los nombres compartidos no podrán tener más de ocho caracteres, seguidos opcionalmente por un punto y entre uno y tres caracteres. Cuando comparta una impresora, el Administrador de impresión truncará automáticamente el nombre de la impresora para crear un nombre compartido que sea compatible con las computadoras con MS-DOS.

Control del acceso a las impresoras

Bajo Windows NT puede realizar el control del uso de cada impresora mediante la configuración de permisos.

De manera predeterminada, todas las impresoras compartidas que se creen estarán disponibles para todos los usuarios de la red. Restringir el acceso a una impresora requiere la modificación de la configuración de permisos de dicha impresora para un usuario o un grupo específico. Para cambiar los permisos de una impresora, es necesario ser propietario de la misma o poseer permiso Control total. Para acceder a la configuración, elija "Permisos" en el menú **Seguridad** del Administrador de impresión.

Las impresoras de red pueden tener cuatro tipos de permisos:

- **Sin acceso**
- **Impresión**
- **Administración** de documentos (permiso para administrar todos los trabajos dirigidos a esa impresora)
- Control total

Estos permisos son acumulativos exceptuando al permiso Sin acceso, que tiene precedencia sobre todos los demás.

Para permitir los siguientes usos de una impresora, conceda el permiso mostrado.

● El permiso autoriza
○ El permiso no autoriza

	Sin acceso	Impresión	Administración de documentos	Control total
Imprimir documentos	○	●	○	●
Controlar las configuraciones de los documentos	○	○	●	●
Detener, reanudar, reiniciar y eliminar documentos	○	○	●	●
Cambiar el orden en la cola de impresión	○	○	○	●
Detener, reanudar y purgar una impresora	○	○	○	●
Cambiar las propiedades de una impresora	○	○	○	●
Eliminar una impresora	○	○	○	●
Cambiar los permisos de una impresora	○	○	○	●

Para crear una impresora en un servidor con Windows NT Advanced Server, debe estar conectado como miembro de uno de los grupos siguientes: Administradores, Operadores de servidores u Operadores de impresión. Para crear una impresora en una estación de trabajo con Windows NT, debe estar conectado como miembro del grupo Administradores o Usuarios avanzados, para dicha estación de trabajo.

De forma predeterminada, los Administradores, los Operadores de impresión y los Operadores de servidores tienen derechos Control total en una computadora (ordenador) con Windows NT. Todos los usuarios pueden administrar sus propios documentos.

Administración de impresoras y de trabajos de impresión

Toda administración directa de una impresora tiene lugar a través del Administrador de impresión. Esto incluye:

- Ver una lista de impresoras y sus respectivos trabajos de impresión.
- Purgar trabajos que estén a la espera de una impresora.
- Mantener en espera o liberar un trabajo de impresión.
- Reiniciar la impresión de un trabajo desde el principio.
- Eliminar un trabajo de impresión.
- Detener un trabajo que se esté imprimiendo en ese momento.
- Interrumpir y continuar trabajando con una impresora.
- Eliminar una impresora.

Se puede administrar un servidor de impresión local o remoto desde cualquier estación de trabajo de la red, siempre que posea los derechos Control total en ese servidor de impresión.

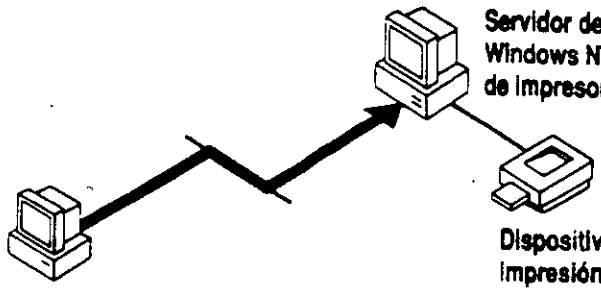
Cuando seleccione un servidor de impresión desde la ventana de Visor de servidores, el Administrador de impresión mostrará el estado de todas las impresoras administradas por esa computadora (ordenador), los documentos en cola para cada impresora y el progreso de todos los documentos que se estén imprimiendo en ese momento. Podrá supervisar varios servidores de impresión e impresoras simultáneamente.

Cualquier usuario de la red puede comprobar el estado de una impresora remota si se conecta con ella. No obstante, únicamente aquellos usuarios que tengan permisos Control total o Administración de documentos para una impresora podrán administrar trabajos de impresión de los que no sean propietarios.

Impresión desde otros tipos de estaciones de trabajo

Las estaciones de trabajo que ejecuten MS-DOS o versiones de Windows para MS-DOS pueden acceder a las impresoras de Windows NT si redirigen sus puertos de salida al *\\servidor\recurso_compartido* apropiado. No obstante, a diferencia de las estaciones de trabajo con Windows NT, estos tipos de estaciones de trabajo deben tener instalado localmente un controlador de impresora. (Consulte el ejemplo en la sección "Configuración de estaciones de trabajo con MS-DOS para impresión en red" al final de este capítulo.)

Las estaciones de trabajo que no tengan Windows NT no pueden acceder a las fuentes y a los formatos disponibles en un servidor de impresora con Windows NT.

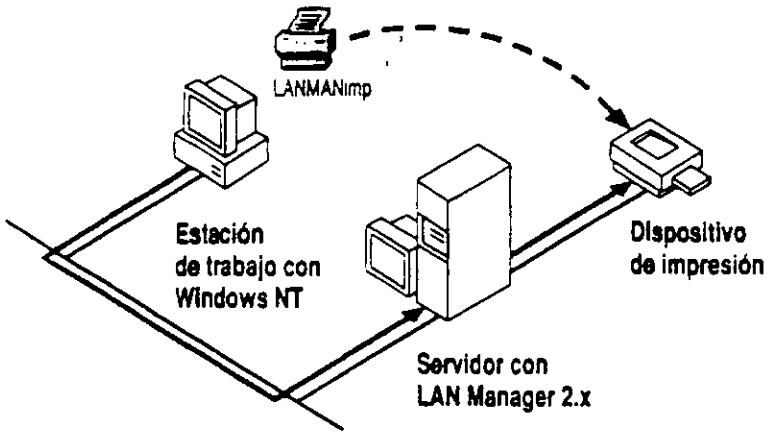


Las computadoras con MS-DOS deben suministrar los controladores de impresoras locales para utilizar las impresoras de Windows NT.

Uso de impresoras administradas por otros proveedores

Su red puede disponer de otros tipos de servidores de impresión; por ejemplo, servidores con LAN Manager 2.x o Novell NetWare. Estos servidores y las impresoras que controlen aparecerán al examinarse la red utilizando el comando **Conectar a impresora** del Administrador de impresión. Sin embargo, puesto que las computadoras (ordenadores) con Windows NT no pueden usar los controladores de impresora de servidores de otros proveedores, cuando se conecte con una impresora de este tipo, el Administrador de impresión le indicará que cree una impresora local e instale un controlador local. Podrá configurar la nueva impresora local de la misma forma que lo haría con cualquier otra impresora.

Solamente los miembros del grupo Administradores o Usuarios avanzados pueden conectar a impresoras que estén administradas por otros proveedores.



Cuando conecta a una impresora administrada por otro proveedor, Windows NT le pide que cree un nombre de impresora local para representar al dispositivo remoto.

Impresión de trabajos

En esta sección se describe exactamente qué ocurre cuando imprime desde una computadora (ordenador) con Windows NT a un dispositivo de impresión. El proceso puede variar dependiendo del tipo de aplicación que esté ejecutando, y dependerá de si la impresión es local o remota.

Puesto que Windows NT es compatible con un gran número de impresoras, fuentes y comandos de gráficos, se reducen al mínimo las complejidades técnicas del proceso de impresión. Al mismo tiempo, el proceso de impresión puede modificarse para las aplicaciones especiales.

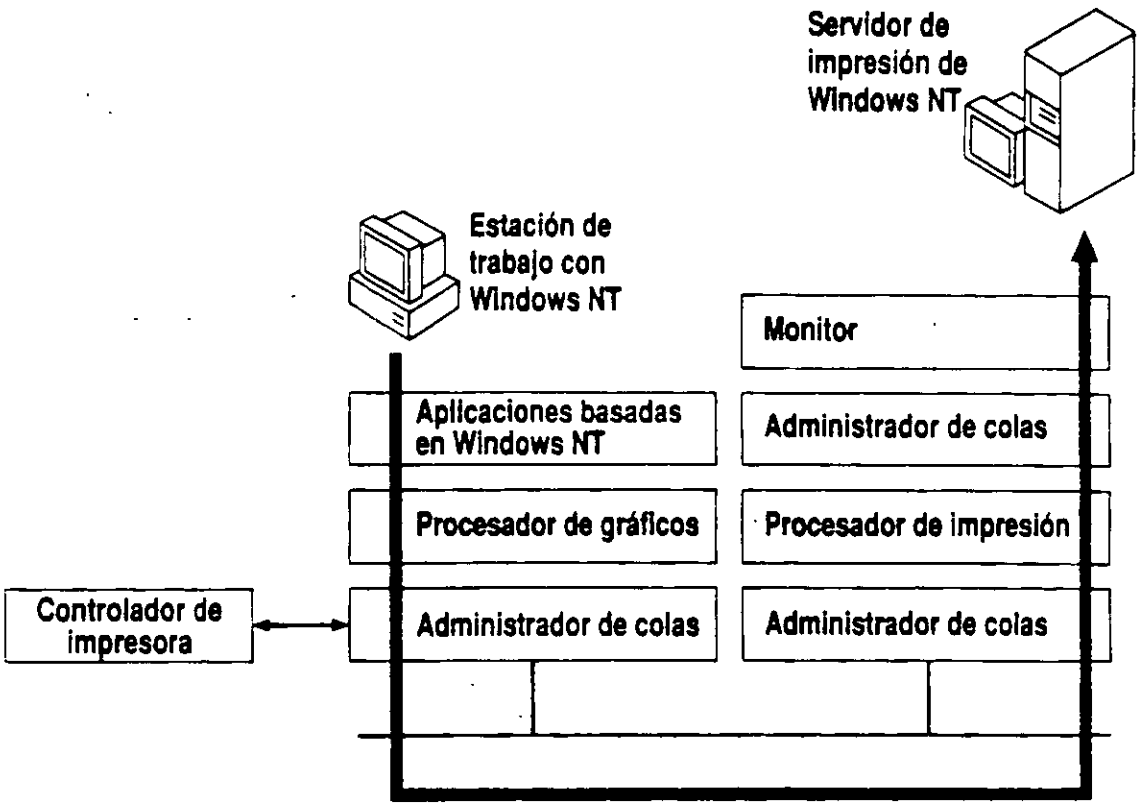
Impresión desde una aplicación basada en Windows NT

Cuando una aplicación basada en Windows NT recibe la instrucción de imprimir en una impresora remota, se inicia la siguiente secuencia de sucesos:

1. En primer lugar, el controlador de impresora correspondiente se copia provisionalmente desde el servidor de impresión a través de la red en la estación de trabajo del usuario. Esto permite a la aplicación de software consultar al controlador la configuración actual de la impresora (resolución, fuentes a color, etc.). La aplicación se comunica con el controlador de impresora mediante el procesador de gráficos.
2. A continuación, la aplicación genera una descripción de la información de salida solicitada, utilizando comandos de *interfaz de dispositivos gráficos* (GDI). Estos comandos especifican toda la información que Windows NT necesita saber acerca del contenido y el formato del documento, pero no indican a la impresora cómo debe imprimir el documento.
3. Después, el *procesador de gráficos* de Windows NT convierte estas llamadas de GDI en llamadas a un *controlador de dispositivo* (DDI), las cuales son traducidas a lenguaje de impresora por el controlador de dispositivo y colocadas en cola de impresión en el servidor de impresión. Desde ahora, el administrador de colas de impresión situado en el servidor de impresión administrará el documento.

   (Observe que para una impresión local, la traducción del controlador de impresora puede efectuarse después de que el trabajo se haya enviado a la cola de la unidad de disco local.)
4. Cuando la impresora de destino esté preparada, el administrador de colas liberará el documento al *procesador de impresión*, el cual, después de comprobar que se trata de un tipo de dato compatible, lo devuelve al administrador de colas.
5. El administrador de cola de impresión transfiere el trabajo al *monitor*, el cual a su vez envía los datos al destino de impresión correspondiente (LPT1, COM1, *\\servidor\recurso_compartido*, etc.).
6. La impresora recibe esta información y genera la información de salida impresa.

En el resto de esta sección se describen estos pasos en mayor detalle.



Procesamiento de gráficos

Cuando inicie el proceso de impresión, la aplicación creará una lista de llamadas a dispositivos gráficos que describirán el documento. El procesador de gráficos tomará estas llamadas y las convertirá en llamadas a DDI. Para poder interpretar correctamente el documento, la aplicación debe solicitar al controlador de impresora correspondiente información de configuración, tal como la resolución de la impresora y las fuentes que estén disponibles. Esta información está disponible porque Windows NT copia provisionalmente el controlador a través de la red a la memoria de la estación de trabajo. Esto sucede al elegirse una impresora nueva o al efectuarse un cambio en la configuración del dispositivo específico. Algunas aplicaciones de tipo WYSIWYG (aplicaciones que imprimen gráficos tal y como aparecen en la pantalla), como Microsoft® Word para Windows™, solicitan el controlador de impresora al iniciar la aplicación.

En el caso de impresión remota, las llamadas a DDI son interpretadas por el controlador de impresora y transferidas como archivos sin procesar al servidor de impresión. (Los archivos sin procesar contienen comandos específicos para la impresora.) En el caso de impresión local, la interpretación puede ocurrir posteriormente si la aplicación puede enviar a cola de impresión un archivo de registro (journal). Los archivos de registro llevan un control de las llamadas a DDI y no contienen comandos específicos para la impresora.

Administración de solicitudes de impresión

La supervisión del proceso de impresión es responsabilidad del administrador de colas. Todas las computadoras (ordenadores) con Windows NT tienen un administrador de colas idéntico que se ejecuta en segundo plano. Durante el proceso de impresión, el administrador de colas de la estación de trabajo cliente transfiere el documento al administrador de colas del servidor de impresión. Este último coordina y planifica todos los trabajos de impresión que lleguen al servidor. Además, enlaza entre sí todos los componentes del proceso de impresión.

Cuando un trabajo de impresión esté en cola, el administrador de colas comprobará si la impresora de destino está ocupada. Cuando el dispositivo esté preparado, el controlador transferirá el archivo al procesador de impresión si se cumplen las siguientes condiciones:

- El dispositivo de impresión está funcionando correctamente y no está en pausa.
- El dispositivo dispone de todo lo necesario para imprimir el trabajo (plumas de trazador adecuadas, papel, etc.).
- El horario de impresión y el volumen de tareas permiten la impresión del documento.
- No hay otros trabajos que posean prioridad superior.

Procesador de impresión

Antes de imprimirse, todos los documentos deben pasar a través de un procesador de impresión. El procesador de impresión de Windows NT es un programa que interpreta el formato de los comandos (tipo de datos) de un documento. Basándose en el tipo de datos, el procesador decide qué procesamiento adicional es necesario. El procesador de impresión también permite la modificación del proceso de impresión.

El procesador de impresión predeterminado de Windows NT admite dos tipos de datos: datos de registro y datos sin procesar. Como se indicó anteriormente, los archivos de registro (journal) contienen llamadas a DDI, mientras que los archivos sin procesar contienen comandos específicos para la impresora.

El procesador de impresión de Windows NT está implementado como una Biblioteca de vínculos dinámicos (DLL). En teoría, el trabajo del procesador de impresión consiste en interpretar los tipos de datos compatibles. Sin embargo, su importancia verdadera consiste en que proporciona acceso al proceso de impresión. El proceso de impresión puede modificarse si se sustituye el procesador de impresión predeterminado de Windows NT por un programa propio. Este programa podría utilizarse para filtrar datos, para crear un diálogo especial con el dispositivo de impresión o para interpretar un tipo de dato nuevo.

Procesamiento en un dispositivo específico

El tipo de dispositivo de impresión determina la manera en que el controlador de impresión administra un trabajo de impresión. Se pueden dar las siguientes situaciones:

- Si el dispositivo de salida es una impresora de líneas, el procesador de gráficos transmite al controlador de impresora una serie de comandos DDI de modo que genere un mapa de bits. Si la impresora no tiene suficiente memoria para el mapa de bits, el controlador realiza un *proceso de banda*, durante el cual el documento se procesa varias veces para generar la imagen completa.
- Si el dispositivo de destino es una impresora PostScript, el procesador de gráficos transmite comandos de DDI que el controlador PostScript convierte en comandos de impresora. La CPU de la impresora efectúa el procesamiento.
- Si el dispositivo de salida es un trazador, el procesador de gráficos transmite comandos que el controlador de impresora utiliza para crear un dibujo de líneas.

Administración de destinos de salida

Un programa de supervisión es responsable de escribir el trabajo de impresión en un destino de salida, como por ejemplo, un puerto local u otro archivo. Windows NT posee tres programas de supervisión. Uno de ellos escribe en los puertos locales, otro en los recursos compartidos de impresión remotos, archivos y canalizaciones con nombre, y el último escribe en las direcciones de la red utilizadas por las impresoras de interfaz de red Hewlett-Packard.

Si el destino es un puerto (LPT1, COM1), el programa de supervisión abre el puerto, escribe los datos y después cierra el puerto. Para los puertos serie, define la velocidad en baudios, la paridad, etc.

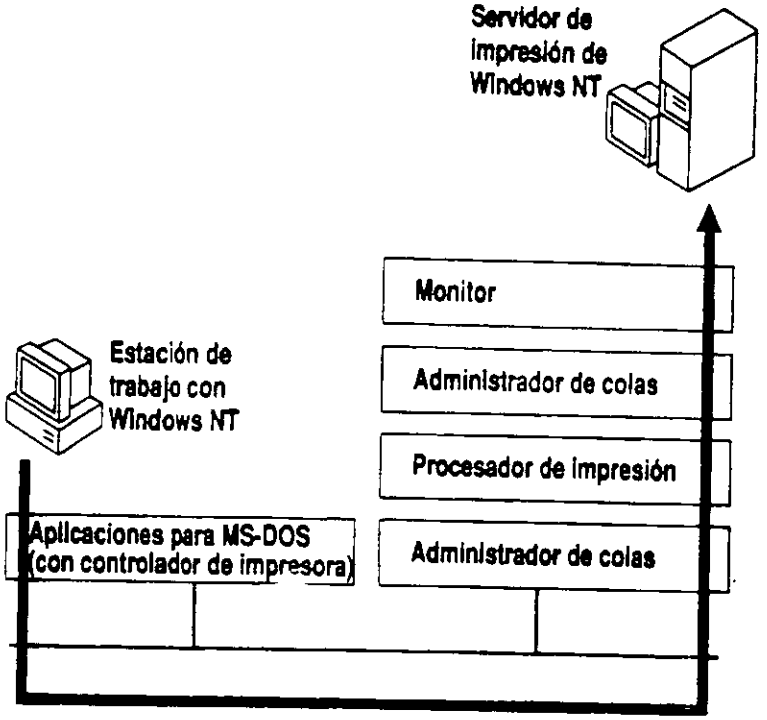
Impresión desde aplicaciones basadas en Windows 3.1 y en MS-DOS

Las aplicaciones basadas en Windows 3.1 que se ejecuten en una plataforma Windows NT se imprimen de la misma forma que las aplicaciones basadas en Windows NT. Estas aplicaciones utilizan controladores de impresión de Windows NT.

Si una aplicación para MS-DOS que se está ejecutando en Windows NT genera gráficos, dichos gráficos deberán ser procesados por la propia aplicación utilizando un controlador de impresora de MS-DOS. El controlador de impresora correspondiente debe estar situado en la computadora (ordenador) local con Windows NT. La información de salida se envía al servidor de impresión mediante la redirección de los puertos paralelo a una dirección de la red.

El proceso consta de los siguientes pasos:

1. Una aplicación basada en MS-DOS crea un documento utilizando un controlador de dispositivo local.
2. El documento se transfiere al servidor de impresión.
3. Cuando la impresora esté preparada, el administrador de colas transfiere el documento al procesador de impresión.
4. El procesador de impresión comprueba el tipo de datos y transfiere el documento al administrador de colas.
5. El administrador de cola de impresión transfiere el trabajo al programa de supervisión, el cual a su vez escribe los datos en el puerto de salida (o en otro destino).
6. La impresora procesa los datos y genera la información de salida.



Ejemplos de configuración de impresión

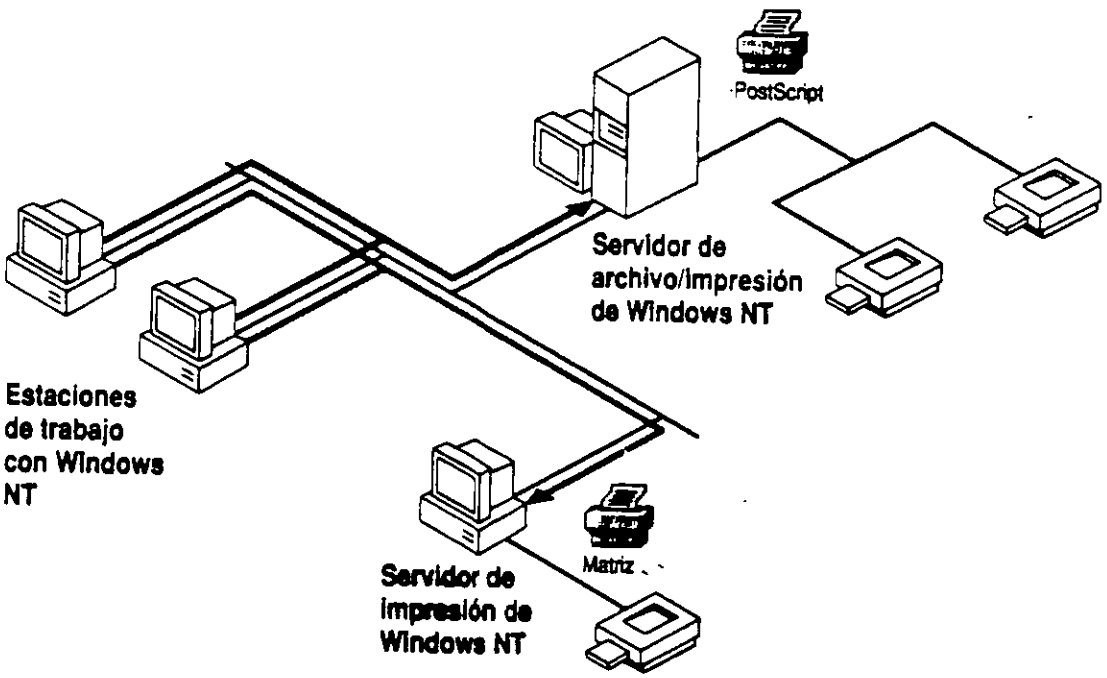
Configuración de un servidor de archivos/impresión para una red pequeña

Supongamos que necesita instalar tres impresoras paralelo (dos impresoras PostScript idénticas y una impresora matriz) en un servidor con Windows NT Advanced Server ya existente.

Puesto que la mayoría de las impresoras matrices son relativamente lentas, procure reservar esta impresora para imprimir facturas, formularios u otros documentos de contabilidad. Para reducir el tiempo de espera para otros trabajos de impresión, configure las impresoras PostScript en un grupo de impresoras.

Si su computadora (ordenador) tiene espacio para tres puertos paralelos, podrá conectar las tres impresoras al servidor. Si no tiene suficiente espacio (o existen conflictos de IRQ), considere la posibilidad de conectar la impresora matriz a una estación de trabajo con Windows NT.

1. Cree dos impresoras utilizando el Administrador de impresión: Matriz y PostScript (puede instalar las dos en el servidor con Windows NT Advanced Server o instalar la impresora PostScript en el servidor con Windows NT Advanced Server y la Matriz en una estación de trabajo con Windows NT).
2. Instale el controlador de impresión correspondiente a cada una. Si todos los dispositivos están conectados al servidor, asigne el puerto LPT1 a Matriz, y LPT2 y LPT3 a PostScript.



3. Utilice el Administrador de impresión para hacer que la configuración de impresión (tamaño de página, memoria, etc.) coincida con la configuración del dispositivo de impresión.
4. Si es necesario, aumente el tiempo de espera para la impresora PostScript. Si se requiere un separador de páginas para los dispositivos PostScript, créelo utilizando la plantilla especial para PostScript.

Configuración de un grupo de impresoras de la interfaz de red

Una empresa desea que configure 12 dispositivos de impresión de interfaz de red HP IIIsi bajo el control de un servidor de impresión. Las impresoras se compartirán entre los empleados que trabajan en el mismo piso de un edificio.

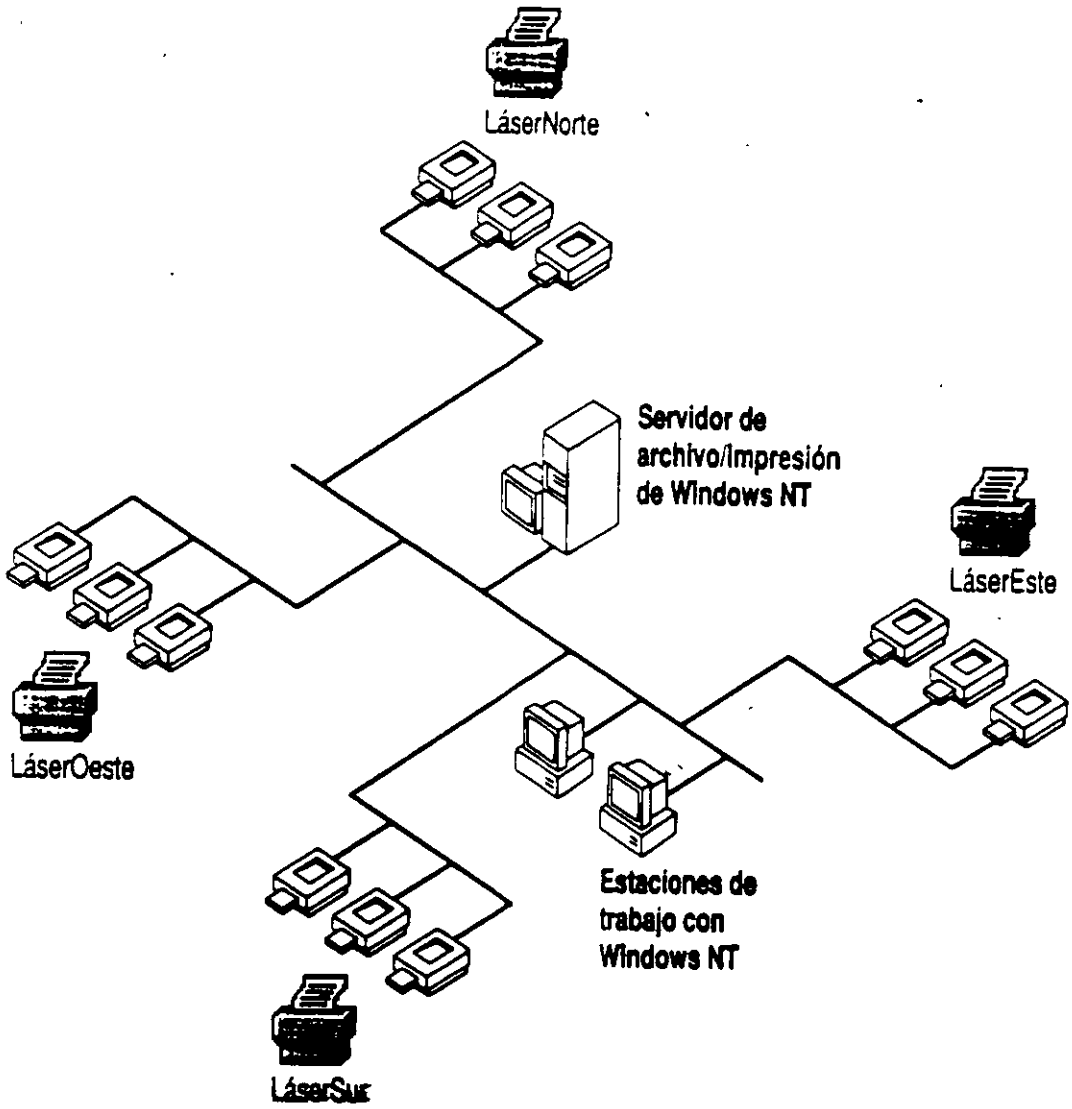
Para evitar que los empleados tengan que dar largos paseos, elija cuatro lugares para colocar las impresoras. Coloque tres impresoras en cada lugar. Coloque el servidor de impresión donde sea más conveniente (recuerde que puede administrar remotamente el servidor). Si la computadora (ordenador) es un servidor con microprocesador x86 dedicado a impresión, son suficientes 12 MB de memoria RAM.

Utilice el icono Red del Panel de control para instalar el protocolo DLC (control de vínculos de datos) en el servidor de impresión. Instale tarjetas de interfaz de red en cada una de las impresoras y, después, ejecute una prueba de autocomprobación de las impresoras para identificar las direcciones de la tarjeta de red.

En el Administrador de impresión, cree las impresoras del servidor de impresión de la siguiente manera:

1. Cree un nombre de impresora para cada uno de los cuatro grupos (por ejemplo, LáserOeste, LáserEste, LáserSur, LáserNorte).
2. Seleccione el controlador de impresora adecuado para cada nombre de impresora. Una impresora podría utilizar un controlador de PostScript, otra podría utilizar un controlador PCL.
3. En el cuadro de destino de impresión, seleccione "Impresoras de red Hewlett-Packard". Aparecerá un cuadro de diálogo en el cual debe escribir un nombre corto para el puerto y elegir una dirección de la lista de direcciones de impresión de la red. Repita este proceso 12 veces, hasta que haya instalado los doce puertos de impresora HP. A continuación, podrá asignar tres puertos para cada LáserOeste, LáserEste, etc. Para asignar más de un puerto, seleccione "Detalles" y luego "Imprimir a puertos adicionales".
4. Modifique las propiedades específicas de cada impresora de modo que reflejen la configuración física de cada grupo de dispositivos.

Cuando un usuario seleccione LáserNorte, la salida puede aparecer en cualquiera de los tres dispositivos de impresión del lado norte del piso. Puesto que las impresoras son idénticas, cada grupo utilizará el mismo modelo de impresión. No obstante, si lo prefiere, podría configurar LáserNorte de modo que emplee papel de tamaño legal, LáserSur de modo que imprima únicamente de noche, etc.

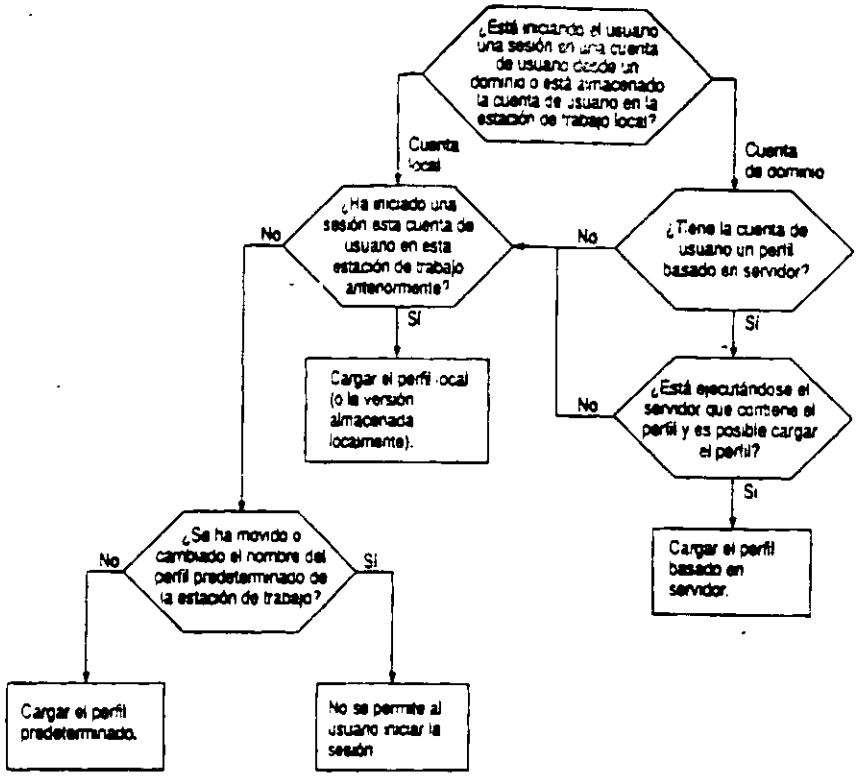


Configuración de estaciones de trabajo con MS-DOS para impresión en red

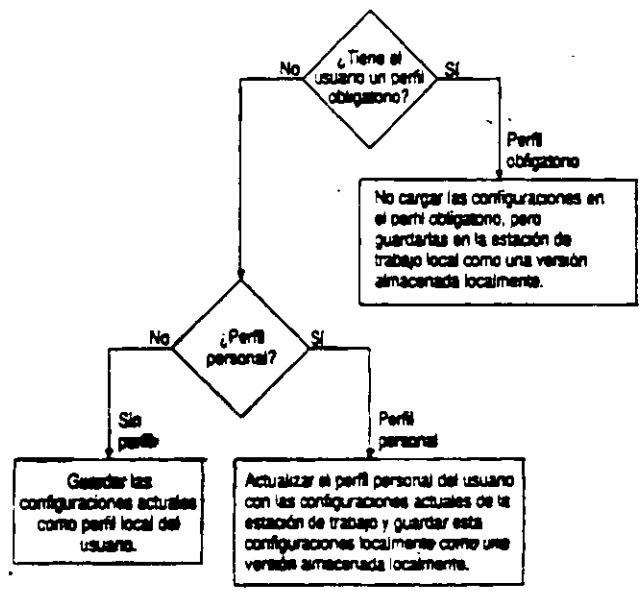
Una empresa acaba de instalar una red de Windows NT. Las estaciones de trabajo de la red incluyen estaciones de trabajo cliente que ejecutan MS-DOS y versiones de Windows para MS-DOS. Estas computadoras (ordenadores) necesitan acceder a una impresora láser administrada por un servidor de impresión con Windows NT.

En cada estación de trabajo con MS-DOS instale el archivo del controlador de impresora de MS-DOS para la impresora láser. Es necesario que cada aplicación que se utilice en la estación de trabajo pueda acceder a este controlador. Puede hacer esto copiándolo en cada directorio de la aplicación. En el símbolo de sistema de MS-DOS, redirija un puerto paralelo libre al nombre compartido de impresora del servidor de impresión con Windows NT (**net use lpt1:** *\\servidor\recurso_compartido*).

Para todas las estaciones de trabajo con Windows basadas en MS-DOS: utilice el icono Impresoras del Panel de control de Windows para instalar el controlador de impresora correcto y asociarlo a un puerto paralelo libre. Después conecte la impresora al nombre compartido y servidor de impresión correspondientes de Windows NT. Es necesario realizar esta acción sólo una vez para todas las aplicaciones basadas en Windows.

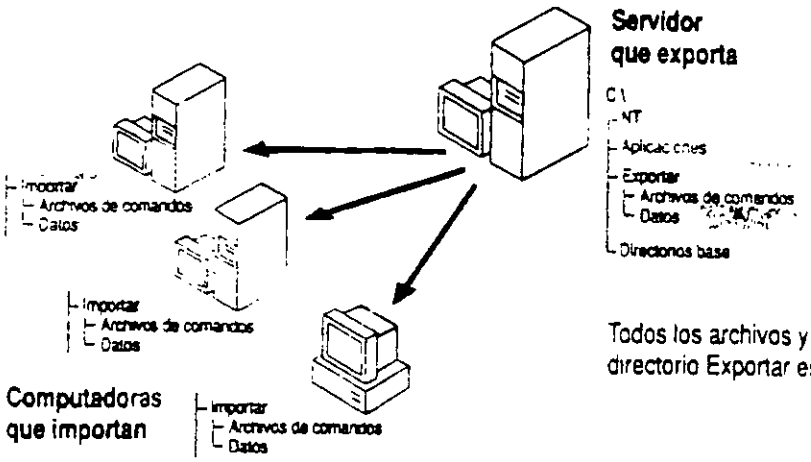


Carga de perfiles.



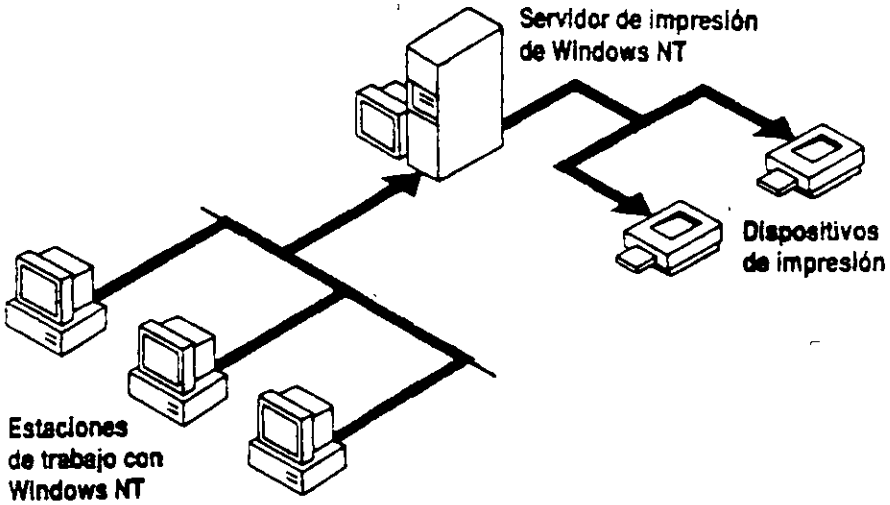
Almacenamiento de perfiles.

WINDOWS NT DUPLICACION DE DIRECTORIO



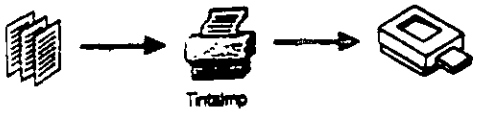
Todos los archivos y subdirectorios del directorio Exportar están duplicados.

Notas:

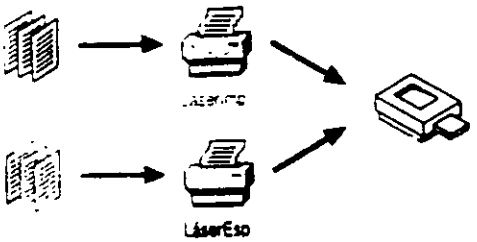

Servidor de impresión
de Windows NT
Dispositivos
de impresión
Estaciones
de trabajo con
Windows NT

Notas:

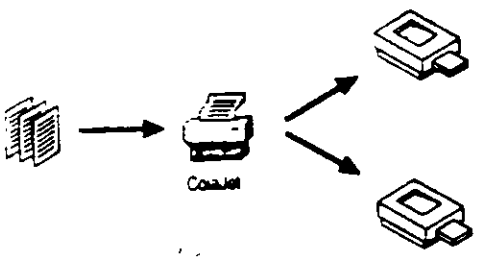
WINDOWS NT PLANIFICACION DEL ACCESO DE LOS USUARIOS A LAS IMPRESORAS



De impresora individual a dispositivo de impresión individual

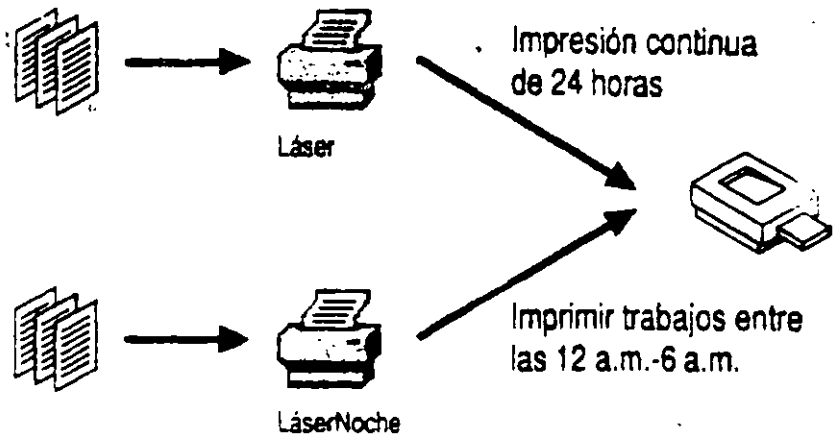


De múltiples impresoras a dispositivo de impresión individual

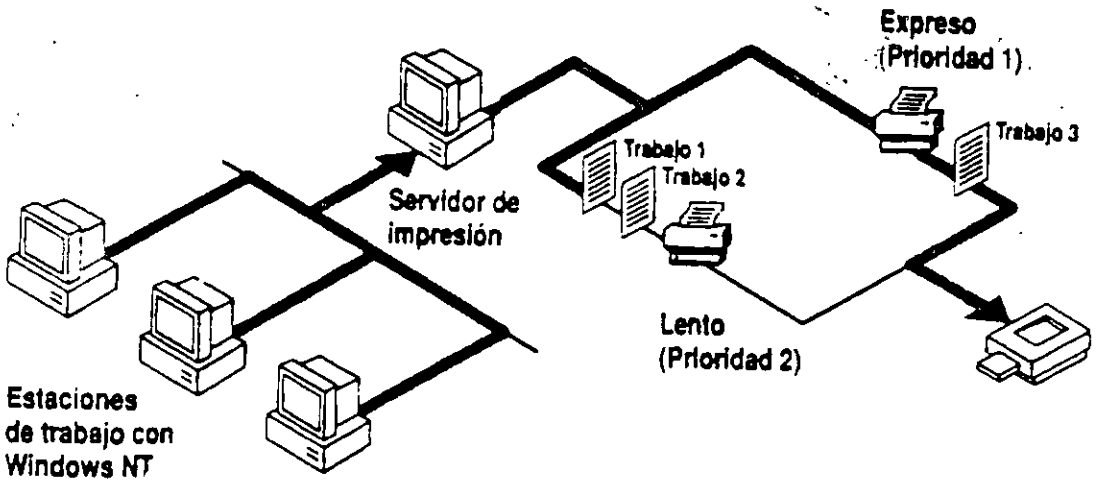


Notas:

WINDOWS NT SUSPENSION DE TRABAJOS DE IMPRESION

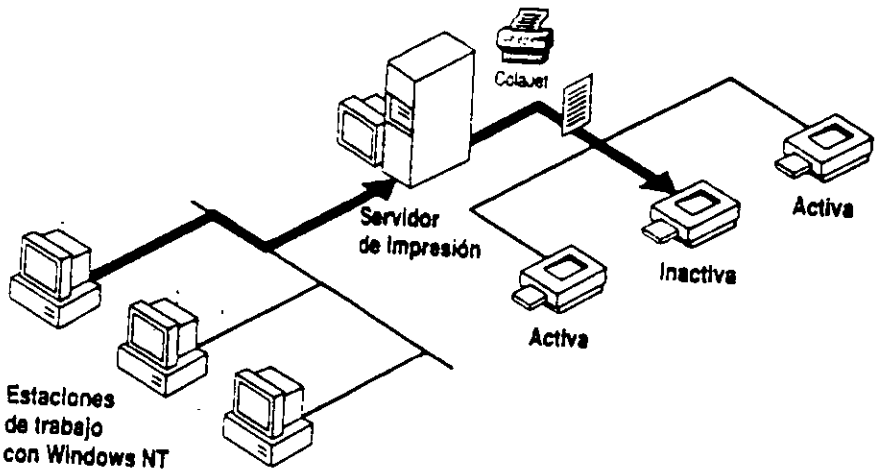


Notas:

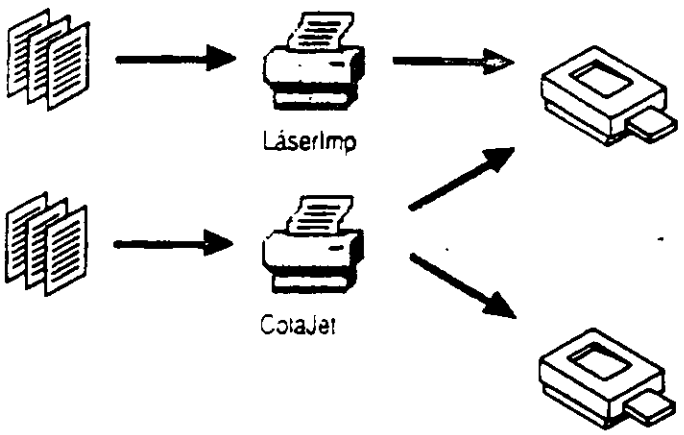

Expreso
(Prioridad 1)
Trabajo 1
Trabajo 2
Trabajo 3
Servidor de
impresión
Lento
(Prioridad 2)
Estaciones
de trabajo con
Windows NT

Notas:

WINDOWS NT USO DE UN GRUPO DE IMPRESORAS

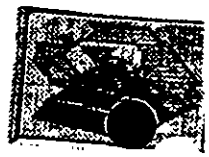


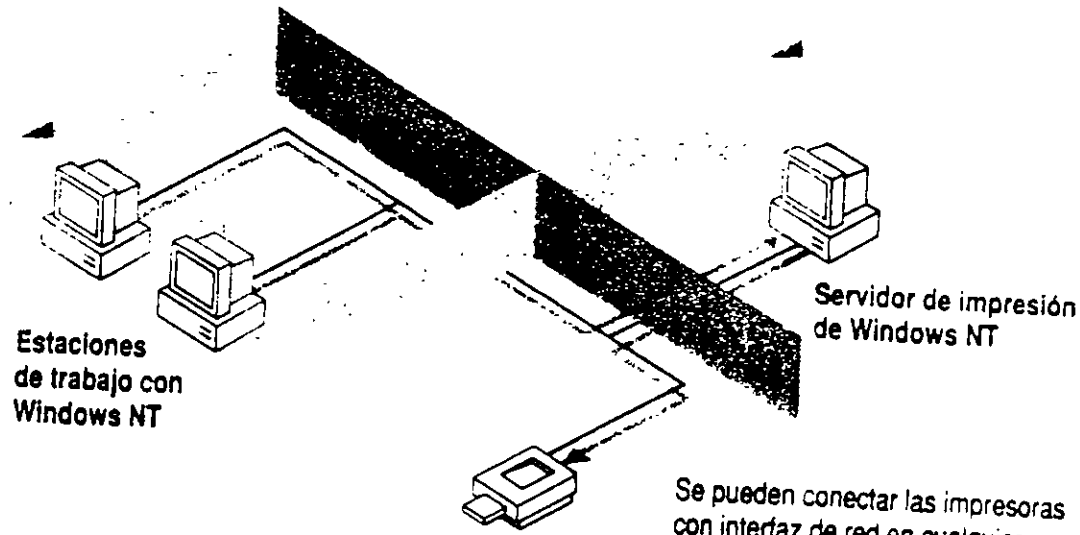
Notas:



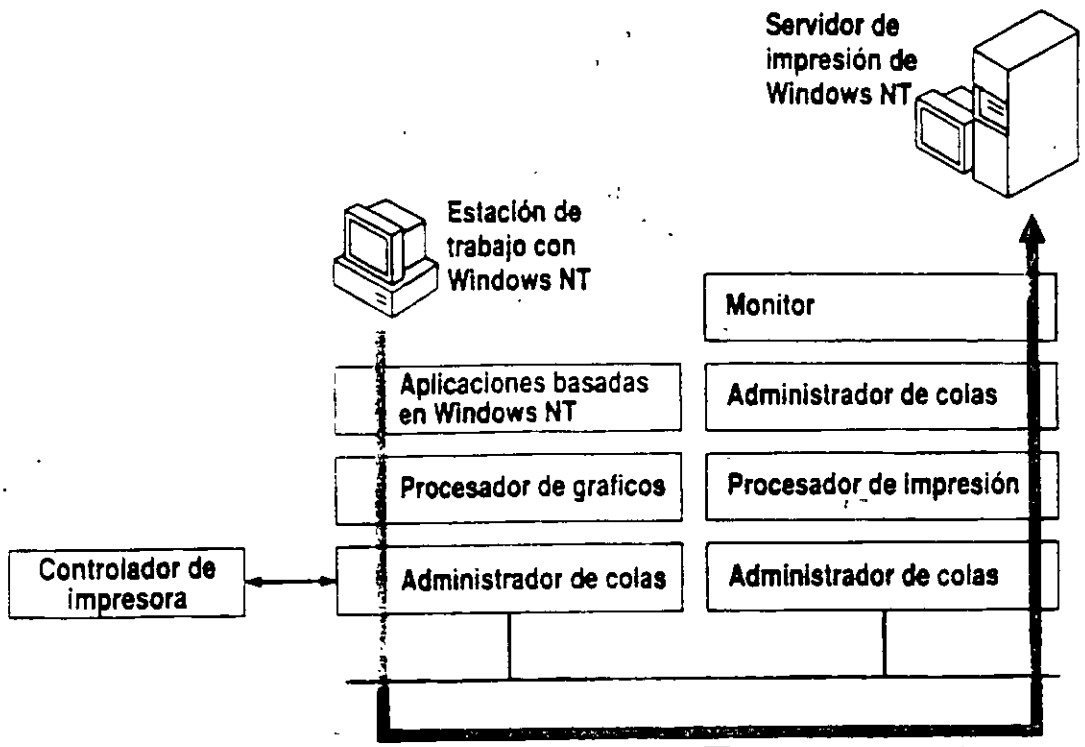
Notas:

WINDOWS NT CONFIGURACION DE IMPRESORAS DE LA INTERFAZ DE RED

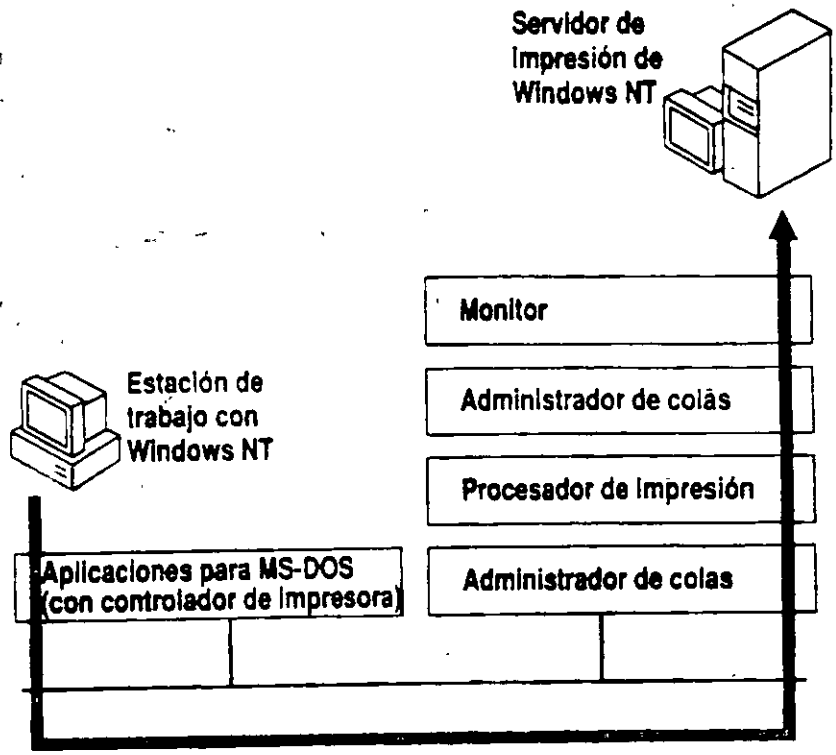




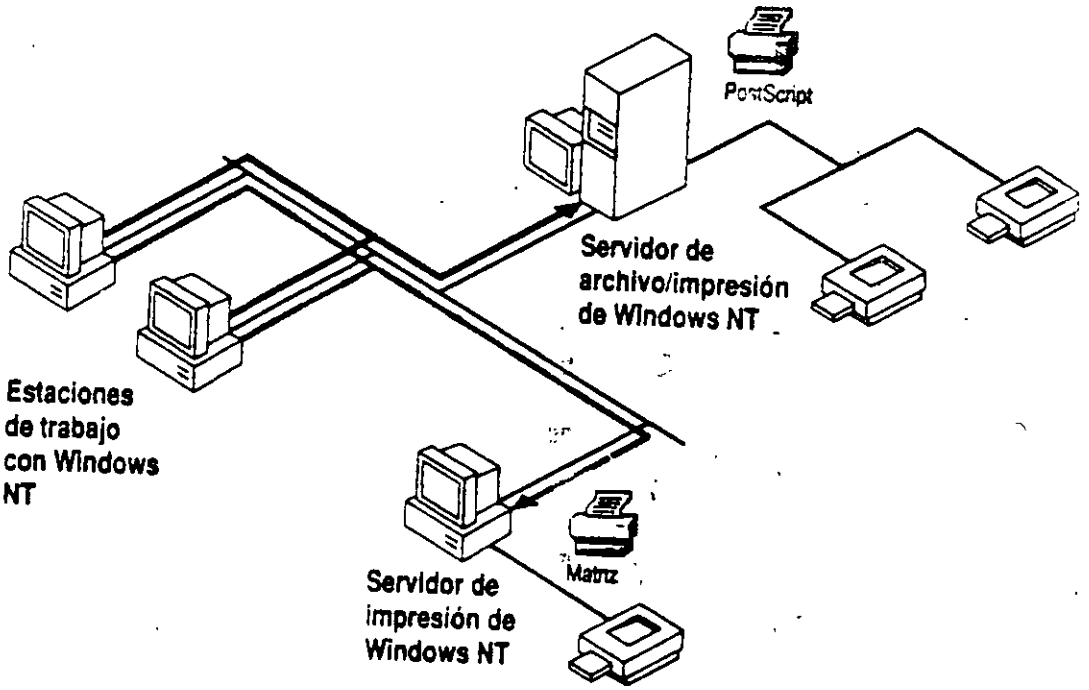
Notas:


Servidor de impresión de Windows NT
Estación de trabajo con Windows NT
Monitor
Aplicaciones basadas en Windows NT
Administrador de colas
Procesador de graficos
Procesador de impresión
Controlador de impresora
Administrador de colas
Administrador de colas

Notas:


Servidor de Impresión de Windows NT
Monitor
Administrador de colas
Procesador de Impresión
Administrador de colas
Estación de trabajo con Windows NT
Aplicaciones para MS-DOS (con controlador de impresora)

Notas:


PostScript
Servidor de
archivo/impresión
de Windows NT
Estaciones
de trabajo
con Windows
NT
Matriz
Servidor de
impresión de
Windows NT

Notas: