Administración y gestión de una red de área local

7

Al finalizar esta Unidad podrás…

- **Conocer las principales tareas y responsabilidades del administrador de red.**
- **Analizar los parámetros de los que depende el rendimiento de una red, proponiendo mejoras.**
- **Diseñar la estructura de servicios de una red de área local y realizar el despliegue de los mismos.**
- **Conocer los criterios de seguridad que garanticen el correcto funcionamiento de los servicios de la red y la confidencialidad de los datos de usuario.**
- **Elaborar la documentación necesaria tanto para los usuarios como para el mantenimiento de la red.**

Introducción

En la Unidad anterior estudiamos la configuración de un servidor para que corriera distintos tipos de protocolos coexistiendo entre sí, analizando las preguntas habituales que se suelen hacer en tiempo de instalación o posteriormente en la configuración del sistema.

Llegados a este punto, una vez que el servidor está en marcha y los distintos protocolos de conexión configurados, tanto en el servidor como en los clientes, es necesaria la definición de los servicios, modos de acceso y parámetros de los sistemas de ficheros de cada servidor o de todo su conjunto; es decir, hay que darle forma al conjunto de servidores y clientes de modo que faciliten su utilización a los usuarios autorizados.

Todas estas funciones son propias de la administración, gestión y seguridad de los sistemas en red de área local.

7.1 El administrador de la red

La persona encargada de las tareas de administración, gestión y seguridad en los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global, es el **administrador de red.** Este conjunto abarca tanto a servidores como a las estaciones clientes, el hardware y el software de la red, los servicios de red, las cuentas de usuario, las relaciones de la red con el exterior, etcétera.

Algunas de estas tareas han sido previamente explicadas: configuración de protocolos, instalación del NOS, diseño e implementación del cableado, etc. No obstante, aparecen funciones nuevas que se apoyan en las anteriormente citadas y que estudiaremos a continuación.

De entre las muchas funciones que se le pueden asignar al administrador de red vamos a destacar algunas de ellas, por la especial importancia que revisten:

- Instalación y mantenimiento de la red. Es la función primaria del administrador. No basta con instalar el NOS en los equipos, sino que además hay que garantizar su correcto funcionamiento con el paso del tiempo. Ello exige tener las herramientas adecuadas y los conocimientos necesarios para realizar esta función.

- En ocasiones, estos conocimientos sólo se pueden adquirir en los departamentos de formación de las compañías suministradoras del hardware y software de las redes o entidades similares. El trabajo propio de mantenimiento puede ser realizado por miembros de la propia empresa, o bien contratar estos servicios con terceras empresas *(outsourcing)*.

- Determinar las necesidades y el grado de utilización de los distintos servicios de la red, así como los accesos de los usuarios a la red.

- Diagnosticar los problemas y evaluar las posibles mejoras.

- Documentar el sistema de red y sus características.

- Informar a los usuarios de la red.

7.2 Organización de la red

Corresponde al administrador de la red, como tarea especialmente importante, la decisión de planificar qué ordenadores tendrán la función de servidores y cuáles la de estaciones clientes, de acuerdo con las necesidades existentes en cada departamento u organización.

Del mismo modo, se ocupará de las relaciones con otros departamentos, grupos o dominios de red, en lo que se refiere a la utilización de los recursos de otros grupos, así como de la comunicación entre los diferentes dominios de gestión.

En la actualidad es común la utilización de servicios que se encuentran en el exterior de la red, es decir, de aplicaciones que se instalan sobre el sistema operativo y que ayudan al administrador a gestionar la red con procedimientos preestablecidos, atendiendo a los eventos que se producen mediante un sistema de alarmas.

Además, los usuarios se benefician de estos servicios remotos de modo transparente, debido al avance que han tenido los protocolos y aplicaciones de capas superiores.

La tendencia en los NOS contempla la posibilidad de utilizar los recursos de red (ficheros, impresoras, programas, etc.) sin preocuparse de su localización física en la red.

A. Servidores de la red

Cuando se establece una estrategia de red es importante, en primer lugar, realizar una buena elección de los servidores con los que se contará. El número y prestaciones de los servidores de red están en función de las necesidades de acceso, velocidad de respuesta, volumen de datos y seguridad en una organización.

Las características técnicas de los servidores de acuerdo con la función que vayan a desempeñar es un tema que ya ha sido estudiado en la Unidad 6.

El número de servidores determina en gran medida la configuración de la red. Efectivamente, si sólo disponemos de un único servidor, éste debe ser compartido por toda la organización. Sin embargo, si se dispone de varios servidores cabe la posibilidad de arbitrar distintas configuraciones.

A pesar de que la carga de trabajo en una organización no exija más de un servidor, puede ser recomendable la existencia de varios servidores, por razones de seguridad, de reparto de flujo de datos, de localización geográfica, etcétera.

En este sentido, los NOS disponen de herramientas de trabajo en red para establecer dominios o grupos que pueden compartir configuraciones de acceso y seguridad. También incorporan capacidades de administración centralizada de los nodos de la red.

Cuanto mayor es el número de servidores de una red, mayor es la carga administrativa, incrementándose también los costes de mantenimiento. Por tanto, en una red no debe haber más servidores que los necesarios.

El crecimiento de la red hace que paulatinamente se vayan incrementando el número de servidores, lo que provoca que ocasionalmente haya que replantearse la asignación de servicios a servidores de modo que se instalen servidores más grandes pero en menor número. A esta operación se le denomina **consolidación de servidores.**

B. Estaciones clientes

En las estaciones de trabajo se han de instalar y configurar todos los protocolos necesarios para la conexión a cuantos servidores necesiten los usuarios.

Por ejemplo, habrá que instalar TCP/IP si se desea hacer una conexión hacia máquinas UNIX, NetBEUI para realizar conexiones sencillas a servidores Microsoft e IPX para la conexión con servidores Novell, aunque ya hemos estudiado en la Unidad anterior que el mundo informático habla, en general, TCP/IP.

Si instalamos más protocolos de los que realmente se utilizarán haremos un consumo excesivo e inútil de memoria central, así como una sobrecarga en el software de red de las estaciones, lo que ralentizará tanto los procesos informáticos como los de comunicaciones.

También hay que asegurarse de que si una aplicación tiene previsto utilizar un interfaz de aplicaciones concreto, por ejemplo, NetBIOS, debe estar instalado, ya que de lo contrario la aplicación de usuario no podrá gestionar las unidades de red remotas. Éste sería el trabajo típico de un **redirector,** como ya se veía en la Unidad anterior.

El administrador debe valorar el modo en que trabajarán los usuarios, con información local o centralizada. Podemos encontrarnos con tres tipos de configuraciones para los clientes:

- Los programas y aplicaciones están instalados en el disco duro local de la estación y no son compartidos por la red. Cada usuario tiene una copia de cada aplicación. Los datos residen también de modo habitual en el disco local, aunque es posible centralizar la información en los servidores.

- Los programas están instalados en el servidor y todos los usuarios acceden al servidor para disparar sus aplicaciones. Por tanto, se instala una única copia de las aplicaciones, lo que ahorra espacio en disco. Hay que tener en cuenta, no obstante, que no todas las aplicaciones permiten esta operativa de trabajo. Los datos de usuario pueden seguir estando distribuidos por las estaciones clientes, aunque también pueden residir en el servidor.

  Hay un caso particular de esta configuración: los clientes ligeros o las estaciones que no poseen disco local (o que poseyéndolo, no lo utilizan para almacenar aplicaciones o datos) y que deben arrancar remotamente a través de la red desde un servidor de sistemas operativos.

- La instalación de aplicaciones distribuidas exige la colaboración del cliente y del servidor, o entre varios servidores, para completar la aplicación. Por ejemplo, una aplicación de correo electrónico consta de una parte denominada **cliente,** que se instala en la estación cliente, y una parte denominada **servidor,** que se instala en el servidor de correo.

  Otros ejemplos de aplicaciones distribuidas son las construidas según la tecnología cliente-servidor,

como las bases de datos distribuidas. Han aparecido nuevas tendencias en la programación de objetos que facilitan la comunicación entre componentes a través de la red. Algunos nombres que nos hablan de estas técnicas son CORBA, DCOM, COM+, ORB, etcétera.

La clasificación anterior está muy simplificada. La realidad es mucho más compleja. Lo habitual en el mundo de los sistemas de red son combinaciones de todas estas posibilidades y, por ejemplo, máquinas que son servidoras con respecto de un tipo de servicio son clientes con respecto de otros.

De la eficacia al diseñar esta estructura de red depende el éxito del administrador de red dando un buen servicio a los usuarios de la red que administra.

C. Conexiones externas a la red

Además de los clientes y servidores de la red, es común la comunicación de datos entre la red de área local y el exterior, ya sea con usuarios de la misma o de distinta organización, pertenecientes o no a la misma red corporativa. Por ejemplo, una red corporativa puede estar constituida por distintas LAN en lugares geográficos distintos.

También es posible la comunicación entre dos LAN pertenecientes a distintas organizaciones. Esta comunicación se realiza a través de redes WAN.

El acceso de un usuario remoto puede ser similar al acceso de un usuario local, disponiendo de los mismos servicios, aunque con rendimientos menores, debido a la inferior capacidad de transferencia de las líneas de transmisión de las redes WAN utilizadas en la conexión. Para ello, basta con disponer de los servicios de conexión y validación apropiados. Éste es el fundamento del **teletrabajo.**

Para poder acceder a estos servicios remotos, es necesario que las LAN posean nodos especializados en servicios de comunicaciones remotas, que también deben estar correctamente configurados.

Las conexiones con el exterior requieren dispositivos especializados que dependen del tipo de conexión y de la WAN que se utilice. Por ejemplo, servidores y clientes RAS o de redes privadas virtuales, interfaces X.25, RDSI, ATM, etc., que serán estudiados en la Unidad 8.

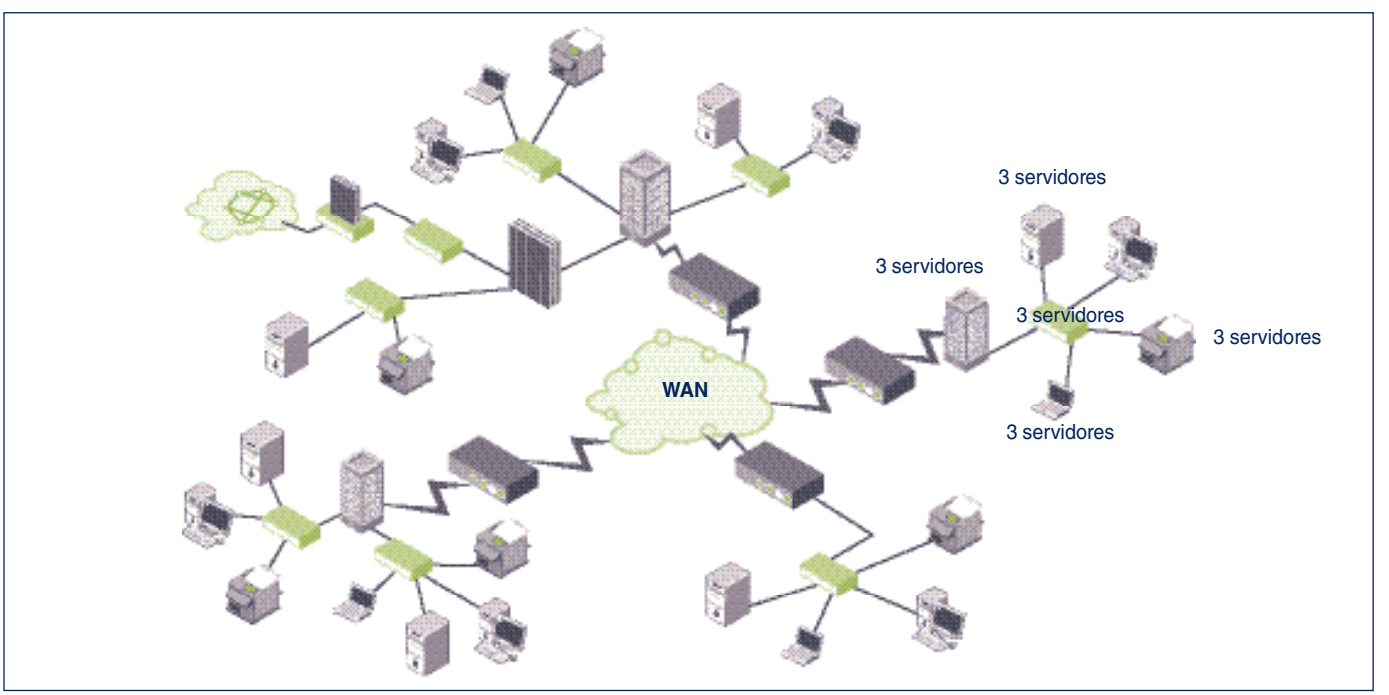

Figura 7.1. *Ejemplos de diagramas de red WAN para una compañía con varias sedes sociales.*

En la Figura 7.1 tenemos un ejemplo de red de área extendida de una compañía distribuida en varias sedes. En estos diagramas se pueden observar las líneas de comunicación a lo largo de todo un amplio territorio, así como los modos de conexión entre los distintos segmentos de red remotos.

7.3 El sistema de acceso a la red

El acceso a la red es el primer aspecto en que debemos fijarnos una vez instalado el software de red. Los servicios que ofrece una estación conectada a la red pueden ser utilizados por cualquier usuario que utilice esa estación de trabajo.

El orden y la confidencialidad de cada puesto de trabajo o proyecto requieren un sistema que garantice que cada persona tenga acceso a sus datos y aplicaciones, evitando que otros usuarios puedan ser perjudicados por el uso indebido del sistema o por la falta de una intención recta.

Todo esto apunta a un nuevo problema que siempre hay que tener en cuenta y que afecta a la seguridad de los sistemas: el intrusismo o *hacking*.

En general, hay tres términos que definen la actuación ilegal oculta en la red:

- ***Hackers.*** Es la persona que trata de «reventar» el sistema operativo, violando su sistema de claves de acceso, con objeto de apoderarse de información reservada o por la mera satisfacción de superar esa dificultad.
- ***Crackers.*** En este caso, se violentan las protecciones anticopia del software.
- ***Phreakers.*** Son individuos que buscan la forma de usar o abusar del teléfono ajeno a su antojo.

Cualquier administrador de sistema o de red tiene que tener en cuenta el posible asalto a la red por parte de personas que se dedican a este tipo de actividades, sabiendo que el ataque puede venir tanto desde fuera como desde dentro de su organización.

El modo de hacer distinciones entre los diferentes usuarios, implica la confección de cuentas de acceso personalizadas y un sistema de validación o autenticación que permite o impide el acceso de los usuarios a los recursos disponibles.

A. Asignación de nombres y direcciones

El primer problema al que hay que hacer frente en el diseño de la estructura lógica de la red consiste en la asignación de nombres y direcciones de red a todos los ordenadores que vayan a convivir con ella. Tanto los nombres como las direcciones han de ser únicos en la red, pues identifican a los equipos.

Una vez que hayamos dado un nombre a cada host, tendremos que registrar éste en algún servicio de directorio, el equivalente a las páginas amarillas de una guía telefónica.

Sobre este tema abundaremos más adelante. Por ahora, basta con aclarar que los nombres de red suelen ser un término alfanumérico, o varios separados por puntos, aunque esto depende del tipo de red.

En el caso de las direcciones ocurre algo parecido. La tecnología de red condiciona el tipo de dirección. Para nuestro estudio, nos centraremos en el sistema de direccionamiento IP, que ya conocemos de Unidades anteriores.

Si el host que pretendemos configurar va a estar en Internet, su dirección IP viene condicionada por la normativa internacional de asignación de direcciones IP.

Sin embargo, si el nodo va estar en una red de área local, podemos asignarle una dirección elegida entre un rango que la normativa IP ha reservado para estos casos y que vienen especificadas en el RFC 1918. Estos bloques de direcciones son del 10.0.0.0 al 10.255.255.255, del 172.16.0.0 al 172.31.255.255 y del 192.168.0.0 al 192.168.255.255.

Además de la dirección IP tendremos que configurar otros parámetros como la máscara. De la asignación de rutas nos ocuparemos con más detalle en la Unidad 9.

B. Cuentas de usuario

Las **cuentas de usuario** son el modo habitual de personalizar el acceso a la red. Así, toda persona que utilice la red con regularidad debe tener una cuenta de acceso.

Para que el control de este acceso sea suficientemente bueno, las cuentas deben ser personales, es decir, dos usuarios no deben compartir la misma cuenta.

La cuenta proporciona el acceso a la red y lleva asociadas todas las características y propiedades del usuario útiles en las labores de administración (Figura 7.2). Las cuentas de usuario suelen tener parámetros semejantes a los que a continuación se describen, aunque cada sistema operativo de red tiene los suyos propios.

- **Nombre de usuario.** Es el nombre único atribuido al usuario y que utiliza para identificarse en la red. Suele ser una cadena de caracteres corta (entre uno y 16 caracteres, normalmente).

- **Contraseña.** Es la cadena de caracteres que codifica una clave secreta de acceso a la red para cada usuario. La contraseña va ligada al nombre de usuario. Proporciona la llave que protege los datos personales del usuario que la posee[1].

- **Nombre completo del usuario.** Es una cadena de caracteres con el nombre completo del usuario. El nombre de usuario suele ser una abreviatura del nombre completo. En este campo se permite un número mayor de caracteres, incluyendo espacios en blanco, para identificar totalmente al usuario. Algunos examinadores de red muestran este nombre al solicitar una inspección de la red.

- **Horario permitido de acceso a la red.** Es un campo que describe las horas y los días en que el usuario tiene acceso a la red. En cualquier otro tiempo el usuario no puede presentarse en la red o es forzado a abandonarla. Por defecto, los sistemas operativos de red permiten el acceso de los usuarios cualquier día a cualquier hora.

- **Estaciones de inicio de sesión.** Describe el nombre de los equipos desde los que el usuario puede presentarse en la red.

- **Caducidad.** Describe la fecha en que la cuenta expirará. Es útil para cuentas de usuarios que sólo requieren accesos por periodos de tiempo concretos. Al desactivarse la cuenta, se impide que otros posibles usuarios (intrusos) se apropien indebidamente de ella y, por tanto, protegen y descargan al servidor de accesos indebidos o indeseados.

- **Directorio particular.** Es el lugar físico dentro del sistema de ficheros de la red en donde el usuario puede guardar sus datos. Al presentarse en la red, el sistema operativo le posiciona en su directorio particular o le concede acceso al mismo.

- **Archivos de inicio de sesión.** Permiten configurar un conjunto de comandos que se ejecutarán automáticamente al inicio de la sesión de red. Están ligados a cada cuenta de usuario, aunque se permite que varios usuarios compartan el archivo de inicio.

- **Otros parámetros.** Algunos sistemas operativos permiten configurar otros parámetros como son los perfiles de usuario, la cantidad de disco de que dispondrá cada usuario, disponibilidad de memoria central, tiempo de CPU, capacidad de entrada/salida, etc. Estos parámetros tienen una especial importancia en grandes sistemas multiusuario. En la Figura 7.2 se pueden ver las fichas que se han de rellenar para la creación de un usuario en el Directorio Activo de Windows.

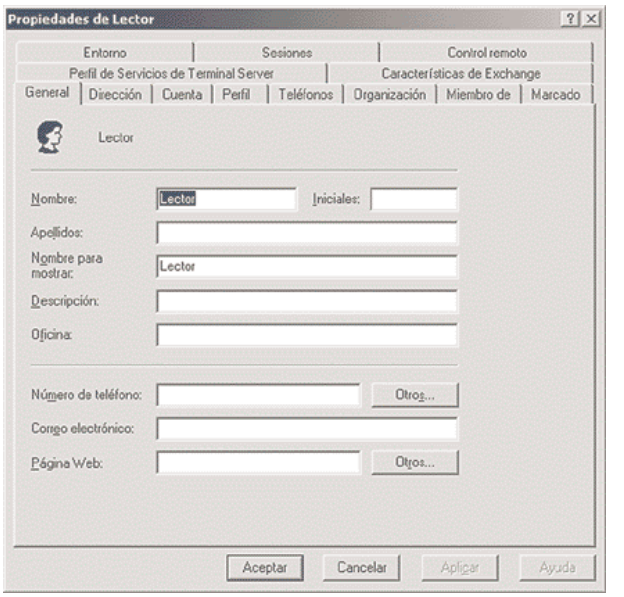

Figura 7.2. *Ficha de creación de un nuevo usuario en un Directorio Activo de Windows.*

Además, el administrador puede establecer una serie de condiciones por defecto asignadas a cada cuenta y gestionadas mediante **políticas** *(policies)*, que facilitan su gestión o que mejoran su seguridad. Entre ellas se encuentran las siguientes:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.

- El usuario no puede cambiar su contraseña.

- La contraseña no caducará nunca.

- La cuenta quedará desactivada en un plazo de tiempo.

- La cuenta se bloqueará si ocurre un número de fallos de presentación consecutivos previamente fijado.

Además de las cuentas que puede definir el administrador de la red, los sistemas operativos de red poseen unas cuentas por defecto con una funcionalidad específica, que normalmente no se pueden borrar, aunque sí modificar y desactivar. Entre estas cuentas se encuentran:

- El **supervisor** (en Novell), **administrador** (en Windows), **root** (en UNIX o Linux), **system** (en VMS), etc. Es la cuenta privilegiada por excelencia y que suele ser utilizada por el administrador del sistema.

- **Invitado** o *guest*. Es una cuenta a la que normalmente no se le asocia contraseña y que carece de privilegios. Sirve para que aquellos usuarios que no

[1] El establecimiento de una buena contraseña es muy importante para la seguridad del sistema. Se recomiendan contraseñas suficientemente largas, con caracteres tanto en mayúsculas como en minúsculas, e incluso combinados con dígitos, espacios en blanco u otros caracteres especiales. No se recomiendan como contraseñas términos que se puedan encontrar en algún diccionario, con independencia del idioma.

tienen cuenta en el sistema puedan acceder a los servicios mínimos, que define el administrador. Por defecto, esta cuenta está desactivada al instalar el sistema operativo de red con objeto de no generar agujeros de seguridad sin el consentimiento explícito del administrador, que regulará los derechos y permisos de estos usuarios invitados.

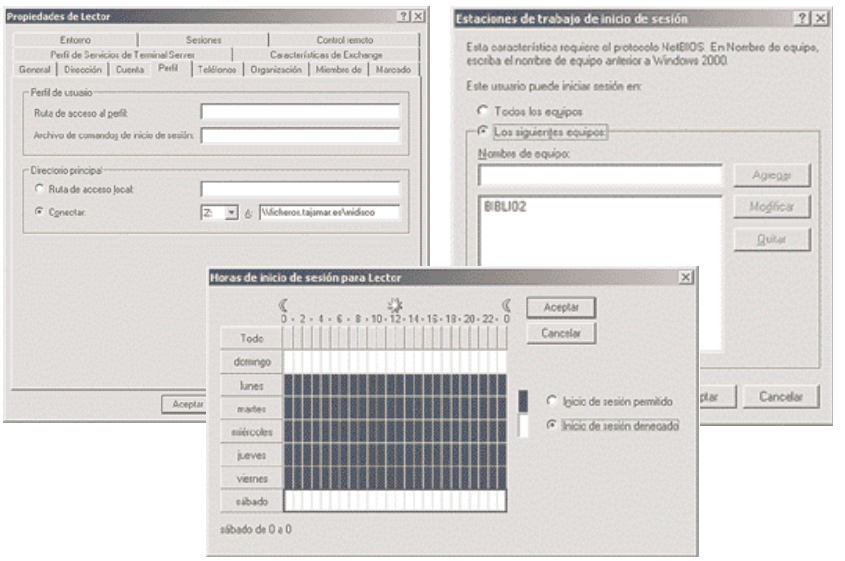

Figura 7.3. *Parámetros habituales en la definición de una cuenta de usuario en Windows.*

En sistemas integrados con dominios o servicios de directorio es posible crear cuentas de acceso tanto en las estaciones locales, para usuarios que sólo se podrían presentar en el sistema local y acceder sólo a sus recursos, o en el dominio o directorio activo. En este segundo caso, las cuentas son válidas para todos los ordenadores que se gestionen desde ese dominio de administración. Ésta es la situación más común en corporaciones grandes y medianas.

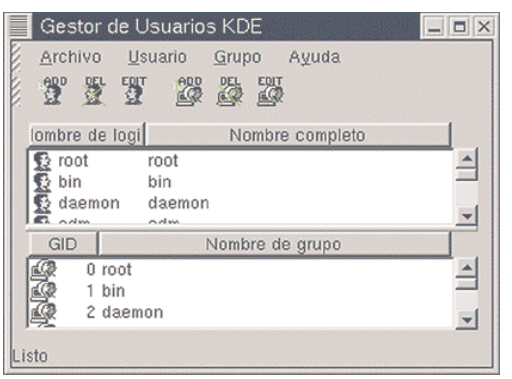

Figura 7.4. *Parámetros habituales en la definición de una cuenta de usuario en un gestor de usuarios con interfaz KDE en Linux.*

C. Derechos de acceso

Una vez que se ha identificado a cada usuario con acceso a la red, se pueden arbitrar sus derechos de acceso. Corresponde al administrador determinar el uso de cada recurso de la red o las operaciones que cada usuario puede realizar en cada estación de trabajo. Ejemplo de estas operaciones son el derecho de acceso a un servidor o a otro equipo a través de la red, forzar el apagado de otro equipo remotamente, reiniciar un equipo, cambiar la hora del sistema, etcétera.

Cada recurso, servicio o utilidad tiene, de este modo, una información asociada que le indica quién puede utilizarlos o ejecutarlos y quién carece de privilegios sobre ellos.

No hay que confundir derechos con permisos:

- Un **derecho** autoriza a un usuario o a un grupo de usuarios a realizar determinadas operaciones sobre un servidor o estación de trabajo.

- Un **permiso** o **privilegio** es una marca asociada a cada recurso de red: ficheros, directorios, impresoras, etc., que regulan qué usuario tiene acceso y de qué manera.

De esta forma, los derechos se refieren a operaciones propias del sistema operativo, por ejemplo, el derecho a hacer copias de seguridad. Sin embargo, un permiso se refiere al acceso a los distintos objetos de red, por ejemplo, derecho a leer un fichero concreto. Los derechos prevalecen sobre los permisos.

Por ejemplo, un operador de consola tiene derecho para hacer una copia de seguridad sobre todo un disco; sin embargo, puede tener restringido el acceso a determinados directorios de usuarios porque se lo niega un permiso sobre esos directorios: podrá hacer la copia de seguridad, puesto que el derecho de backup prevalece a la restricción de los permisos.

La asignación de permisos en una red se hace en dos fases:

a) En primer lugar, se determina el permiso de acceso sobre el servicio de red; por ejemplo, se puede asignar el permiso de poderse conectar a un disco de un ordenador remoto. Esto evita que se puedan abrir unidades remotas de red sobre las que después no se tengan privilegios de acceso a los ficheros que contiene, lo que puede sobrecargar al servidor.

b) En segundo lugar, deben configurarse los permisos de los ficheros y directorios (o carpetas) que contiene ese servicio de red.

Dependiendo del sistema operativo de red, las marcas asociadas al objeto de red varían, aunque en general podemos encontrar las de lectura, escritura, ejecución, borrado, privilegio de cambio de permisos, etcétera.

En redes en las que hay que hacer coexistir sistemas operativos de red de distintos fabricantes, hay que determinar los permisos para cada uno de ellos. A veces los permisos de un tipo de sistema son trasladables fácilmente a otros sistemas, aunque normalmente no coinciden con exactitud. Por ejemplo, en los sistemas de Apple hay tres permisos posibles: ver archivos, ver carpetas y hacer cambios (Figura 7.5, abajo a la derecha).

Sin embargo en Windows NT aparecen nuevos permisos: lectura, escritura, borrado, ejecución, cambio de permiso y toma de posesión. Windows 2000 complica extraordinariamente su sistema de permisos cuando las particiones de disco son NTFS, aunque mantiene compatibilidad con particiones FAT, que carece totalmente de permisos.

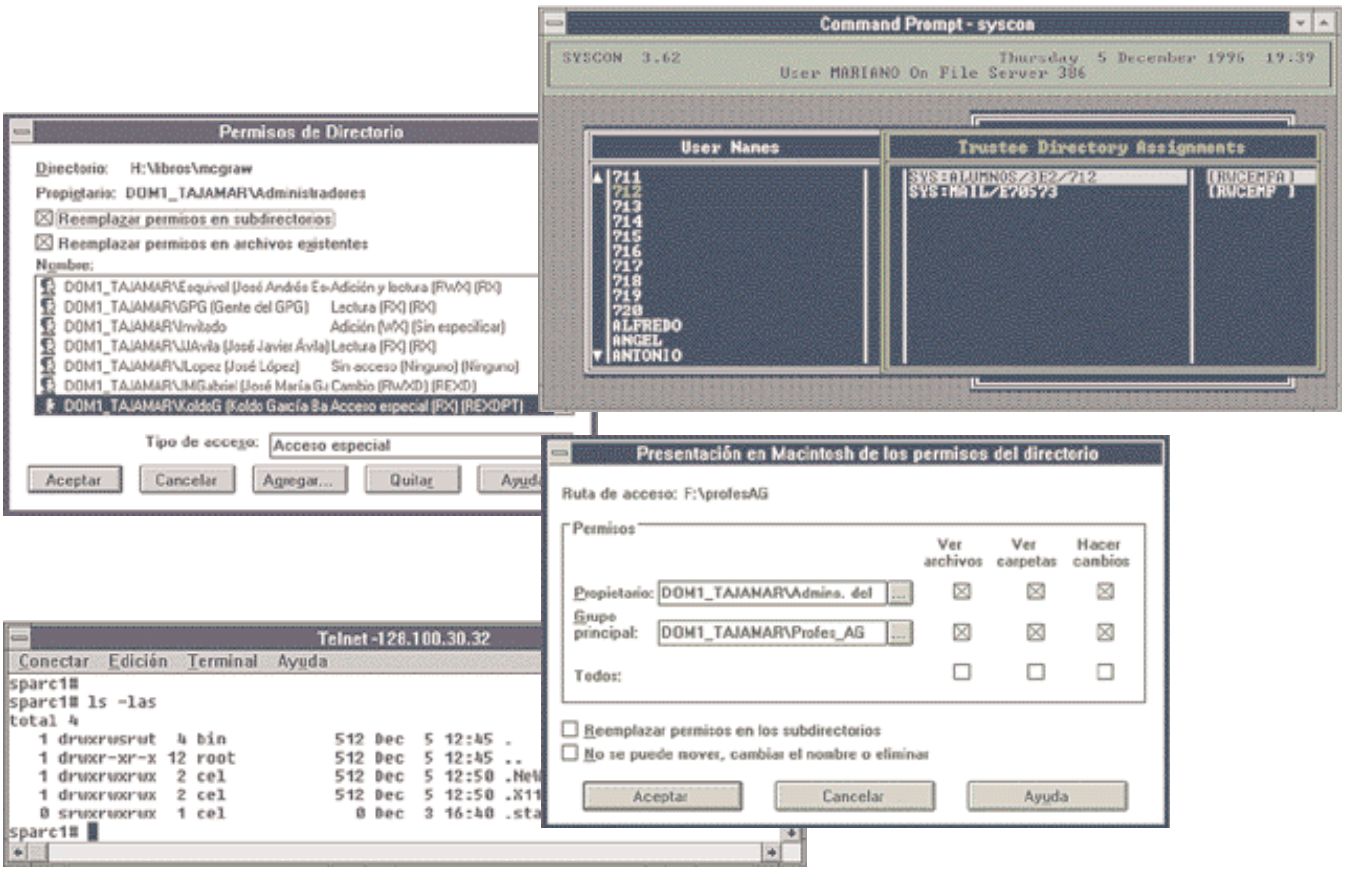

Figura 7.5. *Configuración de privilegios sobre ficheros en distintos sistemas operativos de red.*

D. Cuentas de grupo

Para facilitar las tareas de administración de red, el uso de los servicios o recursos y organizar coherentemente el acceso a la red, existen en los sistemas operativos de red otras entidades de administración denominadas **cuentas de grupo** o simplemente **grupos.**

Una cuenta de grupo es una colección de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo se le asignan automáticamente todas las propiedades, derechos, características, permisos y privilegios de ese grupo. En este sentido, las cuentas de grupo proporcionan una forma sencilla de configurar los servicios de red para un conjunto de usuarios de características similares.

Los NOS tienen unos grupos predefinidos que ayudan a la administración de la red según las necesidades más comunes que se suelen presentar: administradores, operadores de copia, operadores de cuentas, operadores de impresión, usuarios avanzados, usuarios comunes, etcétera.

E. Perfiles de usuario

En ocasiones interesa que el usuario pueda presentarse en más de una estación de trabajo y que esa conexión sea independiente del lugar, haciendo transparente el trabajo en una u otra estación.

Además, puede interesar al administrador tener la posibilidad de forzar el uso de determinados programas o restringir los cambios en la apariencia del interfaz gráfico a ciertos grupos de usuarios. De este modo, los NOS incorporan utilidades que asocian a cada cuenta de usuario o grupo un perfil concreto.

En Novell el ***login script*** general, es decir, el conjunto de órdenes que se ejecutan automáticamente en la presentación, permite asignar los parámetros de inicio que tendrá el usuario. Además de este *login* general, cada usuario tiene un *login script* propio con el fin de personalizar a su medida el comienzo de la sesión.

Las últimas versiones del NOS de Novell incorporan un sistema de administración de red orientado a objetos: todos los elementos de la red se tratan como objetos. Los perfiles de usuario son un objeto más.

Un **objeto-perfil** es un *login script* que se ejecuta entre el *login script* general del sistema y el del usuario. Este sistema de administración se llama **NDS** (*Novell Directory System*). Windows tiene su equivalente en su Directorio Activo.

En otros NOS se pueden encontrar herramientas especializadas en la construcción de perfiles. En Windows, los perfiles contienen todas las preferencias y opciones de configuración para cada usuario: una instantánea del escritorio, las conexiones de red permanentes, las impresoras a las que se tendrá acceso, etcétera.

Los perfiles de usuario pueden estar asociados a una estación de red concreta o bien pueden ser depositados en un servidor de red, de modo que cuando un usuario se presenta, se le asocie el perfil de su propiedad independientemente de la estación por la que acceda a la red: son perfiles móviles.

En sistemas operativos que soportan otros interfaces gráficos como X-Windows para UNIX, OpenVMS, etc., también son posibles las configuraciones de perfiles, aunque son mucho más simples que las de los sistemas basados en Windows o Macintosh.

Sin embargo, el sistema de cuentas y de comandos de inicio (*login* de presentación) es más flexible, es decir, permite al administrador un mayor control sobre los usuarios.

En Windows integrado con su Directorio Activo es posible configurar las cuentas de los usuarios de modo que cuando alguien se presente al sistema desde distintos puntos, incluso remotos, esto se haga de modo que al usuario le sigan tanto su escritorio como sus datos, e incluso, sus aplicaciones (tecnología ***IntelliMirror***).

F. Sistemas globales de acceso

El crecimiento de las redes (en cuanto al número de nodos se refiere) y su organización en grupos de trabajo (subredes, dominios, etc.), así como la integración de NOS de distintos fabricantes, ha llevado a diseñar un sistema de presentación de los usuarios más globalizador.

De este modo, el usuario no tiene que presentarse en múltiples sistemas; basta con que se presente en uno de ellos y la red se encarga de facilitarle el acceso a todos los servicios y sistemas de la red en los que tiene derecho de modo automático.

En algunos NOS, como en Windows, se establecen unas **relaciones de confianza** entre los distintos grupos de red. En las organizaciones en las que el número de nodos es elevado, conviene ordenar todo el conjunto de la red en grupos o dominios. El sistema de cuentas es propio de cada grupo o dominio.

Una **relación de confianza** es un vínculo entre grupos o dominios que facilita la utilización de recursos de ambos grupos o dominios, dando lugar a una única unidad administrativa de gestión de red.

Con el fin de optimizar la organización de la red, es conveniente establecer un dominio maestro centralizador de todas las cuentas de la organización y crear una serie de dominios poseedores de recursos sobre los que establecer las relaciones de confianza necesarias para su utilización.

En la configuración del sistema habrá que indicar el modo en que se transmitirán las contraseñas de los usuarios, que son informaciones extraordinariamente sensibles y delicadas.

Hay varios mecanismos para realizar este procedimiento, que abarcan desde enviar las contraseñas por la red tal y como son escritas por el usuario, sin ningún tipo de protección, hasta la utilización de los más sofisticados sistemas de encriptación, utilizando procedimientos de interrogación y respuesta o servidores de autenticación basados en políticas de certificaciones digitales, como el sistema *Kerberos*, utilizado por muchos sistemas UNIX y Windows.

G. Un ejemplo: el Directorio Activo de Microsoft

El **Directorio Activo,** como su nombre indica, es un servicio de directorio propietario de Microsoft que consiste en una gran base de datos jerárquica (véase Figura 7.6) que organiza todos los objetos necesarios para administrar un sistema Windows en red: usuarios, equipos, datos, aplicaciones, etcétera.

Las principales características del Directorio Activo (DA) son:

- El DA proporciona toda la información necesaria sobre directivas de seguridad y las cuentas de acceso al sistema de cada usuario o grupos de ellos.
- Permite la delegación de la administración, es decir, el administrador puede delegar parte de su trabajo en otras cuentas en las que confía.
- Gestiona un sistema de nombres articulado y jerarquizado en múltiples niveles agrupando todas las cuentas en **unidades organizativas,** que se convertirán en unidades específicas de administración.
- Las relaciones de confianza establecidas entre dos dominios cualesquiera del DA son transitivas.
- Todos los servidores que son controladores de dominio en la misma red de un DA están permanentemente sincronizados, por lo que es fácil la confección de configuraciones de seguridad.

Figura 7.6. *Modelos de estructuras de dominios en un Directorio Activo de Microsoft.*

- El esquema de objetos utilizados por el DA es extensible, es decir, se puede personalizar para que incluya cualquier tipo de información útil al administrador del sistema.
- Lleva un servidor DDNS *(Dynamic DNS)* integrado en el propio DA, lo que le convierte en un servicio extraordinariamente flexible.
- Todas las tareas del DA se pueden automatizar a través de *scripts* o mediante aplicaciones con lenguajes de programación tradicionales orientados a objetos.
- Se permite una gestión basada en políticas o directivas aplicables a las unidades organizativas accesibles mediante consolas de administración (Figura 7.7).

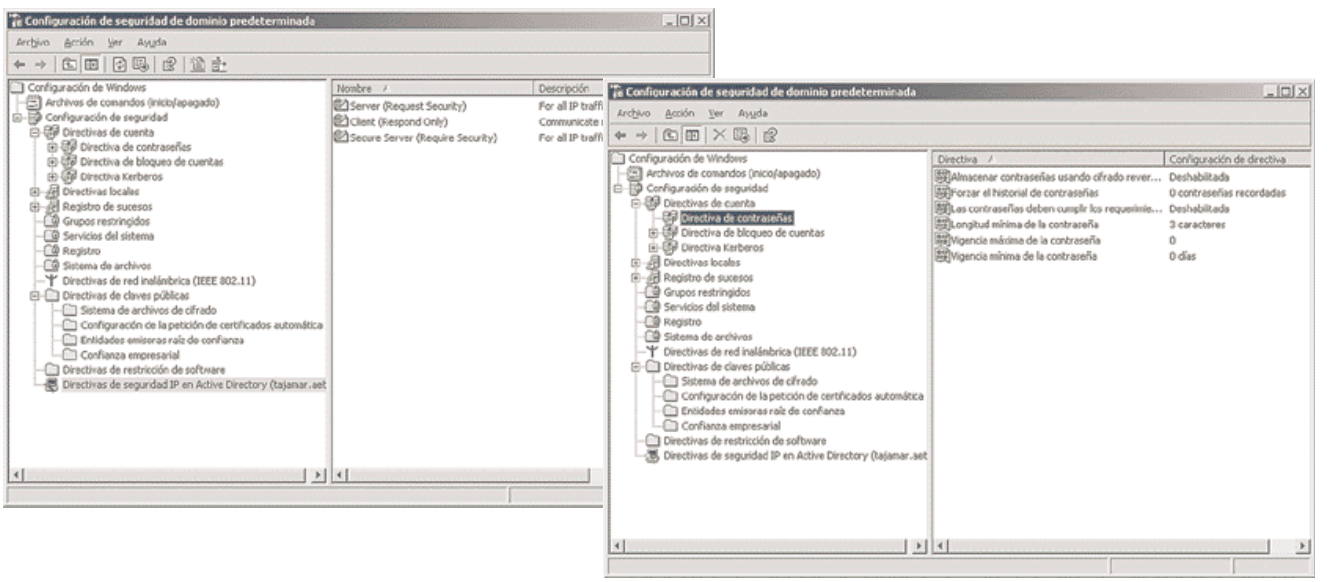

Figura 7.7. *Consola de administración de directivas para un dominio de un Directorio Activo Windows.*

Ejercicio

1 El administrador de usuarios en Linux

Linux aporta varias herramientas para la gestión de usuarios y grupos. Es muy importante que la administración de usuarios esté bien diseñada, especialmente si debe habilitarse posteriormente un buen sistema de permisos de acceso a ficheros, servicios y aplicaciones.

La instalación del sistema operativo crea automáticamente la cuenta del administrador del sistema, que es llamada **root.** La clave de acceso de esta cuenta es generada en tiempo de instalación. Además, Linux crea algunas cuentas y grupos más en tiempo de instalación. Sin embargo, toda la gestión de usuarios debe hacerse posteriormente.

Materiales necesarios

- Un PC con Linux instalado.
- Acceso a la cuenta «root» de administrador en Linux o similar.
- Documentación: manual de instalación de Linux y la utilidad «man» del propio Linux.

Operativa

Linuxconf es una utilidad general para la configuración del sistema operativo. Uno de los elementos que puede gestionar son los usuarios y grupos. También se pueden utilizar otras herramientas como el gestor de usuarios. El gestor de usuarios de Linux es la herramienta por excelencia y específica para la gestión de usuarios y grupos. Es una herramienta de aspecto similar al gestor de usuarios en Windows.

Las anteriores herramientas funcionan en un entorno gráfico X-Windows o similar en Linux. No obstante, este sistema operativo, como cualquier sistema UNIX, permite la gestión de usuarios y grupos desde la línea de comandos. Para ello se pueden utilizar comandos como `/usr/sbin/ adduser` que gestionan los ficheros de cuentas y claves de acceso, que son:

- `/etc/passwd` (fichero de cuentas y claves de acceso).
- `/etc/group` (fichero de grupos).
- `/etc/shadow` (fichero de claves de acceso, si hemos elegido la opción *shadow passwords* en tiempo de instalación).

El aspecto de estos ficheros es el siguiente:

/etc/pwawd	root:/wbUU5z9dJjlo:0:0:root:/root:/bin/bash bin:*:1:1:bin:/bin: daemon:*:2:2:daemon:/sbin: adm:*:3:4:adm:/var/adm: lp:*:4:7:lp:/var/spool/lpd: sync:*:5:0:sync:/sbin:/bin/sync shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown halt:*:7:0:halt:/sbin:/sbin/halt mail:*:8:12:mail:/var/spool/mail: news:*:9:13:news:/var/spool/news:		uucp:*:10:14:uucp:/var/spool/uucp: operator:*:11:0:operator:/root: games:*:12:100:games:/usr/games: gopher:*:13:30:gopher:/usr/lib/gopher-data: ftp:*:14:50:FTP User:/home/ftp: nobody:*:99:99:Nobody:/: postgres:!!:100:233:PostgreSQL Server:/var/lib/pgsql:/bin/bash xfs:!!:101:234:X Font Server:/etc/X11/fs:/bin/false gdm:!!:42:42::/home/gdm:/bin/bash
/etc/group	root::0:root bin::1:root,bin,daemon daemon::2:root,bin,daemon sys::3:root,bin,adm adm::4:root,adm,daemon tty::5: disk::6:root lp::7:daemon,lp mem::8: kmem::9: wheel::10:root	mail::12:mail news::13:news uucp::14:uucp man::15: games::20: gopher::30: dip::40: ftp::50: nobody::99: users::100: floppy:x:19:	console:x:101: utmp:x:102: pppusers:x:230: popusers:x:231: slipusers:x:232: postgres:x:233: slocate:x:21: xfs:x:234: gdm:x:42: Usuarios:*:501:

Tabla 7.1. *Aspecto de los ficheros* `/etc/passwd` y `/etc/group`.

a) Después de familiarizarte con las utilidades de administración de usuarios y grupos, crea un sistema de cuentas para un sistema Linux. Prueba las distintas cuentas. Escribe una guía de operación básica de gestión de usuarios para administradores de sistemas Linux.

b) Realiza esta misma operación sobre sistemas Windows en dos configuraciones: sobre clientes independientes de un dominio y sobre un servidor controlador de dominio en un Directorio Activo.

7.4 Gestión de los servicios

Una vez cubierta la fase de acceso a la red, cada usuario podrá utilizar los servicios a los que tenga derecho de acceso. Sin embargo, una consideración previa del administrador debe ser el modo de disponer los servicios. Una buena elección en el diseño de estos servicios proporcionará un mayor rendimiento de la red.

A continuación estudiaremos los parámetros que hay que tener en cuenta para conseguir mayor eficacia en los servicios de red.

Para la utilización pública de los servicios de red, el administrador debe publicarlos en un servicio de directorio. El servicio más básico es NetBIOS, pero se pueden sofisticar con la tecnología de servicios de directorio más complejos, como NDS o Directorio Activo.

A. Gestión de los discos

En el caso de los servidores de ficheros es importante la configuración de los discos duros; en ellos reside la información centralizada, tanto del NOS como de los datos de los usuarios. Por tanto, la correcta elección del sistema de discos influirá positivamente en la velocidad y en la seguridad del sistema.

En el caso de servidores interesan interfaces rápidos, por ejemplo, discos SCSI, especialmente las últimas versiones de esta tecnología (Ultra/Wide SCSI). En las estaciones de trabajo basta con interfaces IDE o similares. Otros sistemas de red tienen interfaces propietarios para conectar sus discos. Especial importancia cobra la conexión *Fibre Channel* para la conexión de discos con unas especificaciones de velocidad extremas.

Fibre Channel es la tecnología tradicionalmente utilizada para la creación de redes **SAN** (*Storage Area Network*, red de área de almacenamiento), que serán estudiadas más adelante. No obstante, por la importancia que reviste este estándar en la arquitectura de comunicaciones de los sistemas, asimilaremos aquí algunas de sus características.

La tendencia actual de los sistemas de almacenamiento se dirige a hacer transparente a los usuarios el lugar y modo en que residen los datos en el sistema, por ello se puede hablar de una auténtica **virtualización del almacenamiento,** que no es más que un sistema que permite generar y administrar volúmenes virtuales (lógicamente simulados) a partir de volúmenes físicos en disco. A través de este mecanismo se logran eliminar las rígidas características de los volúmenes, dado que los objetos o volúmenes virtuales (lógicos) son más flexibles y manejables. Un volumen virtual puede crecer o disminuir su tamaño sin afectar la información que contiene. Tanto para el usuario como para las aplicaciones, un disco virtual tiene el mismo aspecto que un disco físico. Para el administrador del sistema, los discos virtuales pueden reasignarse sin esfuerzo y sin realizar modificaciones físicas en el hardware ni interrumpir las aplicaciones en ejecución. Adicionalmente, un sistema de virtualización significa una sencillez en la administración del almacenamiento.

Actividad

1. Sobre un sistema Windows, en un volumen del disco duro que no sea el del sistema, crea un conjunto de particiones y formatéalas en distintos formatos: FAT y NTFS. Una vez creadas, arranca el PC con un disquete botable DOS y comprueba que sólo se pueden ver las particiones FAT, al ser DOS incompatible con sistemas de ficheros NTFS. Utiliza el administrador de discos del sistema para probar varias configuraciones con los discos de que se dispongan.

Tomando un sistema Linux, instálale un disco duro nuevo. Prueba las utilidades de creación de particiones y formatea las particiones creadas. Realiza particiones de diferente naturaleza: FAT, ext2, etc. Monta los nuevos volúmenes y prueba su funcionamiento.

Crea una impresora en Windows y Linux para su conexión al puerto paralelo o USB. Añade permisos para que pueda imprimir algún usuario y realiza pruebas de impresión. Cambia algunas propiedades de la impresora y prueba los cambios. Realiza una guía de operación.

Estándar Fibre Channel

Fibre Channel nació en 1988 como una tecnología de interconexión de banda ancha, aunque los primeros productos comerciales no aparecieron hasta 1994. Este estándar consta de un conjunto de normas desarrolladas por ANSI que definen nuevos protocolos para alcanzar transferencias de datos de gran volumen y de muy alto rendimiento.

Su ámbito de utilización es muy variado, pero fundamentalmente se está utilizando en las comunicaciones de alta velocidad por red y en el acceso a los medios masivos de almacenamiento. Se puede aplicar, por tanto, a redes locales, redes de campus, conjuntos asociados de ordenadores (clusters), etc. La distancia máxima permitida por esta tecnología es de 10 Km.

El estándar Fibre Channel es capaz de transportar los protocolos SCSI, IP, IPI *(Intelligent Peripheral Interface)*, HIPPI *(High Performance Parallel Interface)*, los protocolos IEEE 802 e incluso ATM. Actualmente se encuentran en el mercado suficiente número de productos como para poder construir sistemas de comunicación completos: hubs, switches, sistemas, adaptadores y sistemas de almacenamiento.

Originalmente, Fibre Channel se implementó sobre fibra óptica, por eso inicialmente se llamó Fiber Channel. Posteriormente se introdujo también el cable de cobre y cambió su terminología inglesa «Fiber» por la francesa «Fibre», en un intento de desligar la tecnología a la fibra óptica con exclusividad. En las instalaciones reales, se suelen utilizar típicamente distancias de 20 m para segmentos de cobre y hasta 500 m para segmentos sobre fibra.

Con Fibre Channel son posibles tres topologías de red distintas:

- **Punto a punto.** Se utiliza para conectar dos dispositivos, típicamente un ordenador a un periférico o dos ordenadores entre sí.
- **Bucle o *Arbitrated Loop*.** Permite la conexión de hasta 126 dispositivos en bucle cerrado.
- ***Fabric*.** Permite la interconexión de los dispositivos con un comportamiento orientado a la conexión, similar al de una red telefónica convencional.

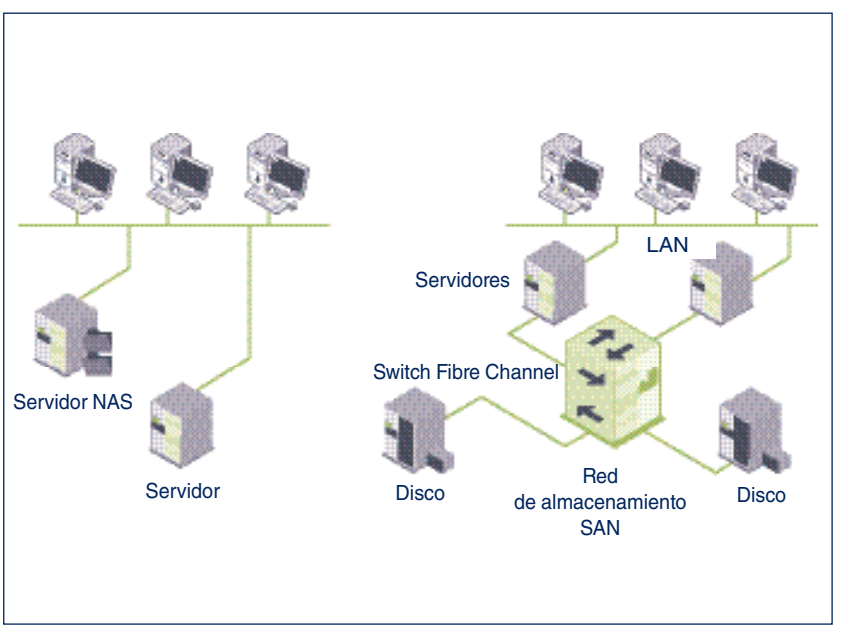

Figura 7.8. *Modelo de almacenamiento NAS (a la izquierda) y SAN (a la derecha).*

La red de comunicaciones y la red de datos

Es frecuente que el volumen de datos a los que se tenga que acceder por una red sea inmenso. En estas situaciones, mover los datos por la red origina fuertes cuellos de botella que hacen que se tengan que modificar las arquitecturas de red para dar respuesta a estas especificaciones tan exigentes, por encima de tecnologías como Gigabit Ethernet o ATM.

Tradicionalmente, el mercado de tecnologías de almacenamiento ha dado varias soluciones que se relacionan a su vez con sendas arquitecturas:

- **Almacenamiento de conexión directa** (*Direct Attached Storage,* **DAS**). Cada estación de red tiene sus discos y los sirve a la red a través de su interfaz de red. DAS es la solución de almacenamiento natural de cualquier ordenador.
- **Almacenamiento centralizado** (*Centralized storage*). Varios servidores o estaciones pueden compartir discos físicamente ligados entre sí.
- **Almacenamiento de conexión a red** (*Network attached storage*, **NAS**). Los discos están conectados a la red y las estaciones o servidores utilizan la red para acceder a ellos. Con servidores NAS la red de área local hace crecer su capacidad de almacenamiento de una forma fácil y rápida sin necesidad de interrumpir su funcionamiento y a un menor coste que si se adquiere un servidor de archivos tradicional DAS (véase Figura 7.8).
- **Redes de área de almacenamiento** (*Storage area network,* **SAN**). SAN es una arquitectura de almacenamiento en red de alta velocidad y gran ancho de banda, creada para aliviar los problemas surgidos por el crecimiento del número de los servidores y los datos que contienen en las redes modernas. SAN sigue una arquitectura en la que se diferencian y separan dos redes: la red de área local tradicional y la red de acceso a datos. Hay, por tanto, dos redes: un *backbone* de transmisión de mensajes entre nodos y una estructura de switches de canal de fibra (duplicados por seguridad) y de muy alto rendimiento que conecta todos los medios de almacenamiento. Los entornos en que está indicada una solución SAN son aquéllos en que los backups son críticos, en los clusters de alta disponibilidad, en las aplicaciones con bases de datos de gran volumen, etc. Los equipos SAN más modernos pueden alcanzar velocidades de transmisión de datos desde los discos de varios Gbps (véase Figura 7.8).

Los switches de una red SAN suelen utilizar la tecnología Fibre Channel y frecuentemente están duplicados para garantizar el servicio. Como veíamos, están apareciendo otras tecnologías que no siguen este estándar, por ejemplo, la tecnología iSCSI, que utiliza protocolos TCP/IP para transportar por la red comandos propios de la tecnología SCSI.

B. Gestión de impresoras

No todos los usuarios de una red tienen a su disposición dispositivos de impresión en sus ordenadores locales. Las redes ofrecen la posibilidad de compartir estos dispositivos, de modo que las inversiones sean más asequibles. Las redes de área local permiten a los clientes la conexión a las impresoras disponibles en toda la red y a las que tengan derecho de acceso. Incluso es posible la conexión a impresoras que estén conectadas a redes de otros fabricantes. Por ejemplo, desde una estación Windows se puede imprimir en una impresora conectada al puerto paralelo de un servidor NetWare.

La labor del administrador de red se simplifica cuando el sistema de impresoras está centralizado en los servidores, ya que tendrá un mayor control sobre los recursos de impresión. El administrador puede controlar los servidores de impresión, las impresoras remotas, las colas de impresoras, etcétera.

Existen servidores de impresión expresamente dedicados a este tipo de tareas, gestionando todas las tareas de impresión con arreglo a unos parámetros concretos: velocidad de impresión, calidad de impresión, privilegios, prioridades, costes, etc. Otras configuraciones, más comunes, para los servidores no dedicados se limitan a servir las impresoras que se les conectan a sus puertos de comunicaciones.

Conceptos relativos al sistema de impresión de red

Describiremos aquí los términos y conceptos más utilizados para la descripción de un sistema de impresión en red:

- **Dispositivo de impresión.** Son los dispositivos físicos (hardware) que son capaces de producir un documento impreso. Son dispositivos de impresión las impresoras de papel, las filmadoras de película fotográfica, los plotters o trazadores gráficos, etcétera.

- **Impresoras lógicas.** Son los dispositivos lógicos (software) que nos proporciona el NOS y que conectan con el dispositivo de impresión a través de un puerto de comunicaciones.

- **Controlador de impresora.** Es un programa que convierte el documento electrónico de su formato original a un formato legible por el dispositivo de impresión. Existen varios lenguajes descriptores de páginas (PDL) legibles por los dispositivos de impresión como PCL de Hewlett-Packard, PostScript de Adobe, Interpress de Xerox, etcétera.

- **Cola de impresora.** Es un sistema gestor de los documentos que permanecen a la espera para ser impresos. En algunos sistemas operativos de red, las colas de impresora coinciden con las impresoras lógicas, siendo aquéllas una característica técnica más de éstas.

- **Administrador de trabajos en espera o *spooler*.** Es un sistema que gestiona las colas de impresora, es decir, es el encargado de recibir trabajos, distribuirlos entre las impresoras, descargarlos de la cola una vez impresos, avisar de la finalización de la impresión, informar de posibles errores, etcétera.

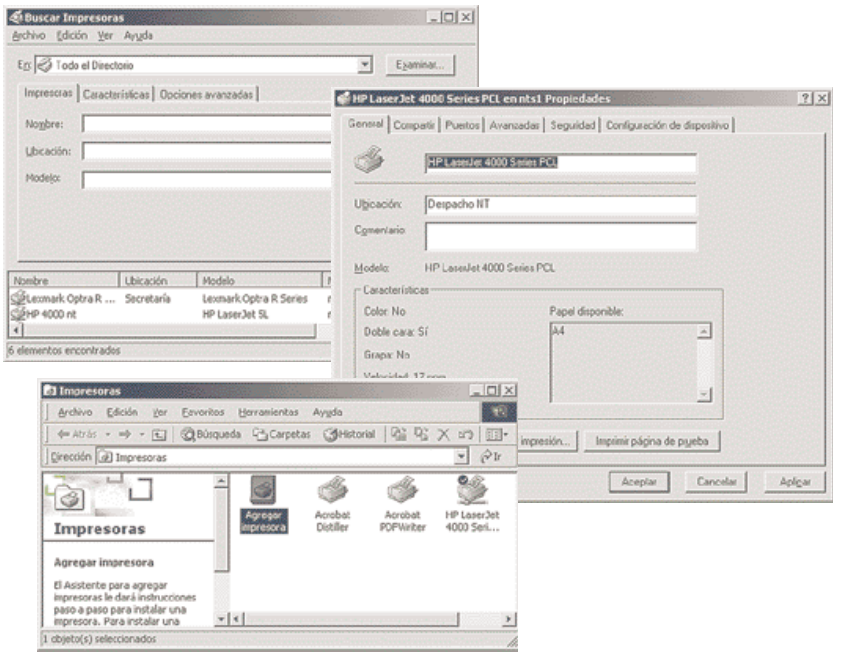

Figura 7.9. *Entorno de impresoras en Windows: arriba, conexión a una impresora de red; abajo, administrador de impresoras desde donde se dispara el asistente de conexión; a la derecha, ficha de propiedades de la impresora.*

Para conseguir un rendimiento elevado y equilibrado de los dispositivos de impresión, estos parámetros deben estar correctamente configurados en el NOS (Figura 7.9). Como con cualquier otro recurso de red, también aquí son aplicables los permisos de uso y su administración remota. Para ello, es recomendable la utilización de los documentos de ayuda que proporciona el fabricante del NOS.

Diseño del sistema de impresión

Un buen diseño del sistema de impresión redunda en una mayor eficacia del sistema, así como en un abaratamiento de los costes de instalación, al poder reducir el número de impresoras sin perder funcionalidad. Articularemos el diseño del sistema de impresión en diversas fases:

a) **Elección de los dispositivos de impresión.** Deben ser elegidos de acuerdo con las necesidades de los usuarios. Es útil considerar los siguientes elementos antes de tomar las decisiones de instalación:

- Pocos dispositivos de impresión de alto rendimiento frente a muchos dispositivos de rendimiento moderado.
- Número de páginas totales que se van a imprimir y velocidad de impresión de las mismas.
- Calidad de impresión, elección de color o blanco y negro, tamaño de la página impresa, etcétera.
- Conectividad del dispositivo de impresión. Impresoras conectadas a un puerto paralelo o USB de un servidor, impresoras conectadas directamente a la red, etcétera.
- Tecnología de impresión. Las impresoras pueden ser matriciales, láser, de inyección de tinta, de sublimación, etcétera.
- Protocolos de comunicación. En el caso de las impresoras de red, hay que tener en cuenta el protocolo que utiliza para que los clientes realicen la conexión con la impresora.
- Costes de los equipamientos de impresión y de sus consumibles, costes por página impresa, etcétera.

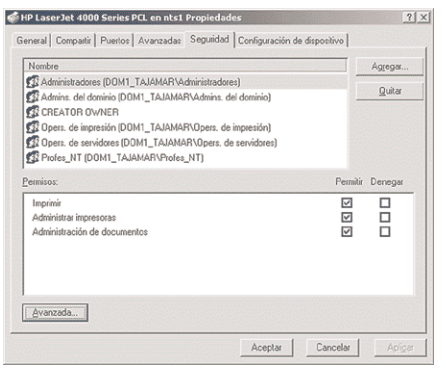

Figura 7.10. *Asignación de permisos para un recurso de impresión.*

b) **Asignación de las impresoras a los equipos.** Seguidamente, hemos de distribuir las impresoras por toda la red teniendo en cuenta las características de los equipos. Se puede considerar lo siguiente:

- El proceso de impresión consume muchos recursos de CPU; por tanto, las impresoras servidas a la red deben residir en máquinas con suficiente potencia si se prevé que la impresión va a ser frecuente.
- Además, normalmente, cada trabajo por imprimir debe almacenarse en el disco duro del servidor de la impresora, con lo que debemos asegurarnos que tendrá suficiente espacio libre.
- Las impresoras deben estar geográficamente distribuidas por toda la organización de acuerdo con unos criterios. Hay empresas que prefieren centralizar todas las impresoras con el fin de evitar ruidos, especialmente en el caso de impresoras matriciales o de línea, mientras que otras prefieren una distribución por departamentos o, incluso, la asignación de una impresora por cada usuario.

c) **Acceso a las impresoras.** Para definir el acceso a las impresoras, hemos de considerar dos partes bien diferenciadas:

- La asignación de impresoras lógicas a dispositivos de impresión. Pueden darse los casos de una a uno, una a varios y varias a uno. Todos los sistemas admiten la asignación uno a uno. El resto de asignaciones son posibles en función de los sistemas operativos: frecuentemente es necesario instalar software de terceras partes.
- La asignación de los derechos de acceso para cada usuario o para cada grupo (Figura 7.10).

Algunos NOS disponen de herramientas de administración para lograr que las impresoras disparen trabajos en determinadas circunstancias. Por ejemplo, a partir de cierta hora nocturna, una impresora matricial inicia la impresión de unos recibos que han sido confeccionados y enviados a la impresora durante el día.

Del mismo modo, se pueden asignar prioridades a los diferentes trabajos, de modo que se altere el orden en que los trabajos serán seleccionados por el *spooler* para ser impresos. Además, cuando una cola atiende a varios dispositivos de impresión, el primero que quede libre recibirá el siguiente de entre todos los trabajos pendientes en esa cola.

Creación de una impresora lógica

El proceso de creación de una impresora lógica suele ser un procedimiento asistido por el NOS, que facilita la tarea del administrador (Figuras 7.9 y 7.10). En general se puede dividir en tres fases:

- **Selección de la impresora y del software controlador.** En esta primera fase se le indica al NOS qué tipo de impresora queremos instalar, así como cuál será el controlador que debe utilizar para la gestión de la impresora. Cada NOS admite una amplia variedad de impresoras, que además se actualizan frecuentemente.

  No obstante, si la impresora es posterior a la fecha de fabricación del NOS, es posible que el fabricante de la impresora tenga que suministrarnos un disquete o CD-ROM con el software controlador propio del sistema operativo sobre el que pretendemos realizar la instalación.

  Conviene pasarse periódicamente por las sedes web de los fabricantes del hardware de que disponemos por si han liberado nuevas versiones de los *drivers* con errores corregidos, mejores prestaciones o mayor funcionalidad.

- **Establecimiento del nombre de la impresora.** Consiste en la asignación de un nombre que identificará unívocamente a la impresora. En algunos NOS, también se proporcionan otros datos informativos como la situación geográfica en donde se ubicará el dispositivo impresor, el nombre del propietario, etcétera.

- **Elección de los parámetros por defecto de la impresora** (Figura 7.11). Aquí se especifica el tamaño del papel, la resolución, la conversión de color a gris, etcétera.

Impresoras IPP

IPP o *Internet Printing Protocol* (Protocolo de Impresión Internet) es el modo de utilizar tecnología web para transmitir los ficheros que se quiere imprimir a una impresora compatible con esta tecnología.

IPP utiliza HTTP para realizar estas transmisiones, lo que la hace muy interesante ya que puede atravesar los cortafuegos con los que las organizaciones se protegen sin necesidad de abrir nuevos puertos de comunicación que aumenten la superficie de exposición a riesgos innecesarios.

En la parte izquierda de la Figura 7.12 pueden verse las propiedades del puerto de una impresora conectada a la red y compatible con IPP; en la parte derecha aparece una página web con la administración de la impresora.

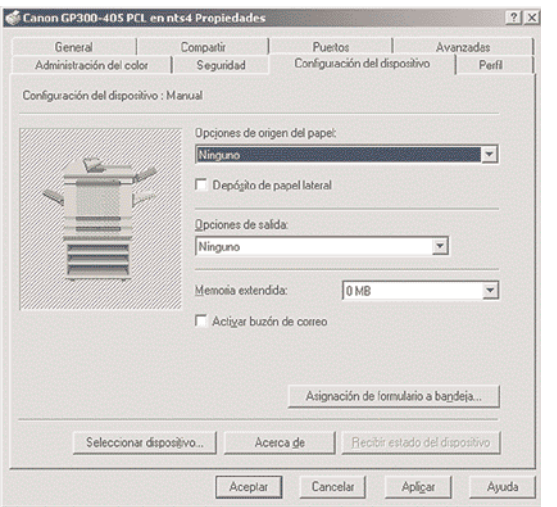

Figura 7.11. *Configuración de una impresora de red instalada en un entorno Windows.*

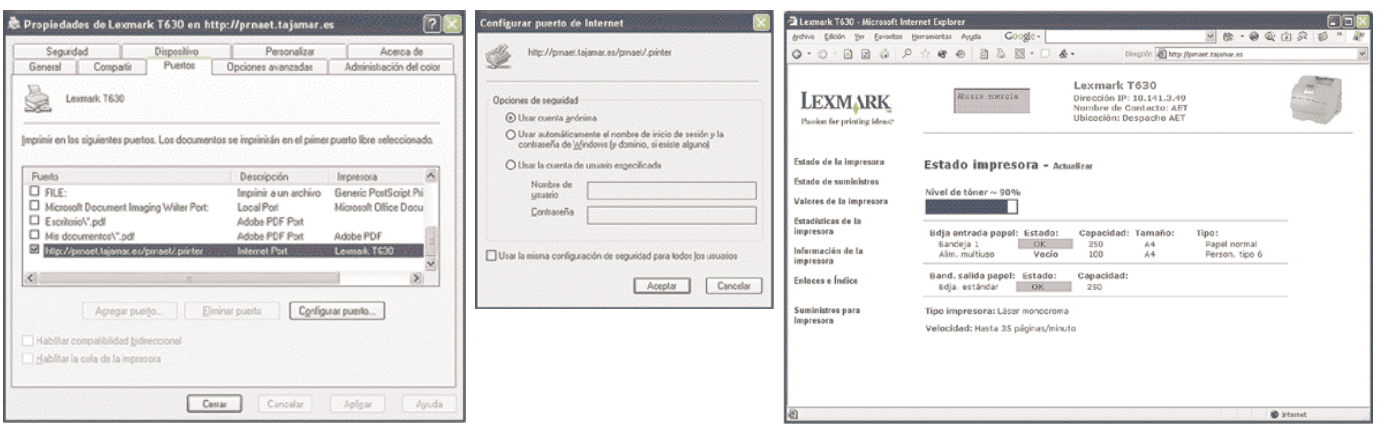

Figura 7.12. *Configuración del puerto de una impresora IPP y página de administración.*

Windows incorpora IPP para que las impresoras definidas en sus servidores puedan ser gestionadas a través de IPP. Como el protocolo de transporte de información se basa en HTTP, es indispensable que el servidor tenga instalado IIS, el servidor web de Windows. Se puede acceder a las impresoras una vez instalados el componente IPP y el servidor web a través de la dirección http://nombre_servidor/printers (véase Figura 7.13).

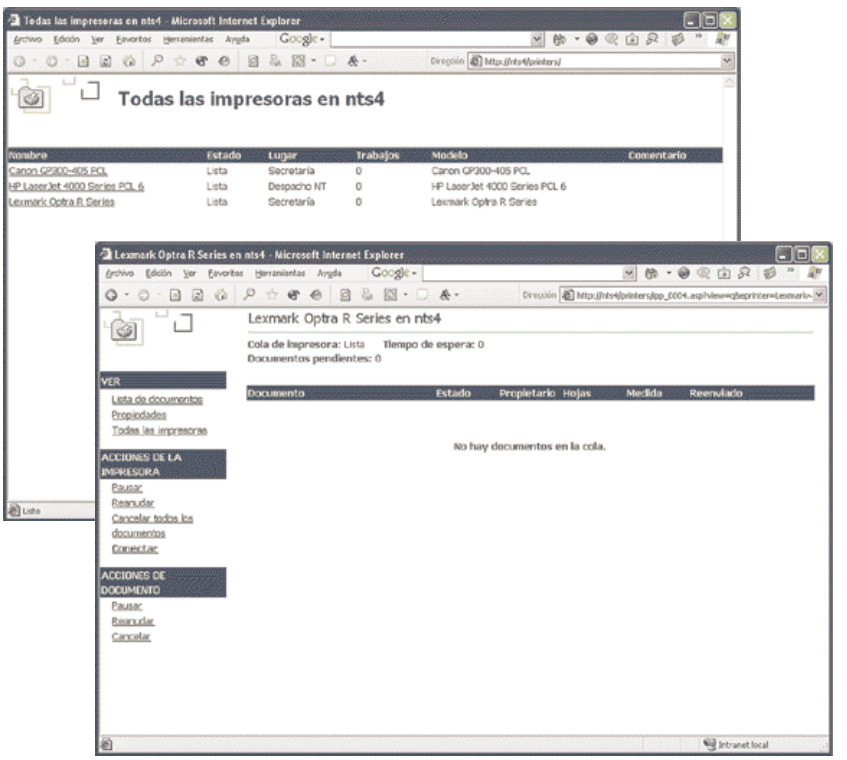

Figura 7.13. *Configuración desde Windows de una impresora gestionada vía web.*

Actividad

2 Crea una impresora en Windows y Linux para su conexión al puerto paralelo o USB. Añade permisos para que pueda imprimir algún usuario y realiza pruebas de impresión. Cambia algunas propiedades de la impresora y prueba los cambios.

Asigna permisos a los distintos usuarios de la impresora y verifica que su funcionamiento es correcto.

Sirve la impresora a la red y comprueba que desde otros clientes que se puedan conectar a la impresora se puede imprimir por ella a través de la red.

Ahora, sobre el sistema Windows, instala el protocolo de impresión por Internet, es decir, el protocolo IPP. Comprueba que puedes gobernar la impresora desde el explorador de Internet mediante el protocolo IPP.

C. Configuración del correo electrónico

El correo electrónico es una de las aplicaciones de red más utilizadas en las redes de área local corporativas. Proporciona un medio de comunicación eficaz y libre de errores entre los usuarios de la red y puede dejar constancia escrita de los mensajes intercambiados.

Una aplicación completa de correo electrónico consta de un cliente y un servidor. El servidor gestiona los mensajes de modo que lleguen a sus destinatarios. Para ello, a veces ha de pasar los mensajes a los sistemas de correo de otras redes (*relay* o retransmisión de mensajes). Por ejemplo, si una corporación tiene dos delegaciones situadas en distintas ciudades y quieren conectar sus sistemas de mensajería electrónica, necesitarán un servidor de correo que se encargue de traspasar los mensajes en una y otra dirección, de modo que todos alcancen su destino. Además, los servidores de correo contienen los buzones de sus usuarios, que almacenan sus mensajes en espera de ser leídos.

El cliente de correo electrónico es el interfaz que permite a los usuarios la edición, visualización y la impresión de mensajes, así como otras funciones propias de los sistemas de correo.

El administrador de red debe encargarse de la gestión de cuentas de correo, de situar la oficina de correos en un lugar accesible a todos los usuarios con derecho a correo y de velar por el correcto funcionamiento del servicio de correos.

La operativa que permite enviar un mensaje de correo electrónico tiene los siguientes pasos:

a) Se ejecuta la aplicación cliente de correo electrónico, presentándose en el sistema a través de su nombre de usuario y su clave de acceso.

b) Si en el momento de la presentación hay correo en el buzón del usuario, el sistema le informa de la existencia de nuevos mensajes por si desea leerlos.

c) Seguidamente, se redacta el mensaje que deseamos enviar. Algunos sistemas de correo permiten editar el texto utilizando procesadores de texto comunes en el mercado ofimático. También se permite la incorporación de ficheros externos al mensaje en cualquier formato (ficheros adjuntos).

d) A continuación, se rellenan los parámetros de envío: nombre del destinatario, dirección del destinatario (si se encuentra en otra red), solicitud de acuse de recibo, prioridad del mensaje, etcétera.

e) En la fase final se procede al envío del mensaje, dejando al sistema la responsabilidad de la entrega a su destinatario una vez lo haya convertido a un formato de envío adecuado.

Además, el sistema de correo permite otras operaciones básicas sobre los mensajes recibidos: hacer copias en forma de ficheros independientes, responder al remitente, responder a todos los miembros de la oficina de correos, eliminar un mensaje, imprimirlo, almacenarlo en alguna carpeta pública o privada, encriptarlo, certificarlo, etc. En el caso de que se disponga de un servidor de correo, la configuración es más compleja, pero mucho más versátil.

D. Configuración del servicio de fax

Algunos sistemas operativos permiten la conexión de un módem/fax interno o externo que habilitan las conexiones de fax tanto en envío como en recepción. La configuración de un fax exige tres pasos:

a) **Preparación del módem/fax con los parámetros adecuados.** Se debe configurar el módem para adecuar la velocidad de transmisión y recepción, el puerto serie o USB al que se conectará, etc. Normalmente, esta configuración se realiza a través de **comandos Hayes.** En la actualidad casi todos los módems analógicos (y también gran parte de los digitales a partir de la implantación de RDSI) incorporan las normas fax, por lo que se les llama **fax-módem.**

b) **Configuración del software en el NOS.** La mayor parte de las aplicaciones de fax configuran el software como si se tratara de una impresora más que, en vez de imprimir en un papel, envía los datos a través de una línea de teléfono. En recepción, el fax recoge la información en un fichero gráfico, que seremos capaces de visualizar por un monitor o de imprimir por una impresora. El software suele incorporar utilidades para rotar la imagen, cortarla, añadir notas, etc. Para el usuario, el fax no es más que una cola de impresora y su gestión es similar a la descrita para la gestión de estas colas.

c) En una tercera fase, **el sistema de fax se puede integrar dentro del sistema de mensajería electrónica de la red,** por ejemplo, en un servidor de mail. Esta opción se utiliza, sobre todo, para la recepción centralizada de faxes, con el servidor como encargado de su distribución a los destinatarios apropiados. De este modo, los mensajes se reparten eficazmente entre los usuarios de la red, independientemente de que provengan de correo electrónico interno, correo de Internet o mensajes gráficos en formato facsímil.

Se empiezan a instalar sistemas en los que se integra la voz (teléfono), el fax y el correo electrónico en un único sistema de mensajería electrónico que contiene todas las pasarelas necesarias para que pueda haber intercomunicación entre sistemas tan distintos: nos referimos a la convergencia de tecnologías de mensajería.

Actividad

3 Sobre un sistema Windows instala el servicio de comunicación por fax. Observarás que si tienes definido un módem-fax, el servicio de fax verá a éste como una impresora: cualquier documento que sea impreso por esa impresora lógica seguirá el protocolo de comunicación por fax. Prueba su funcionamiento.

7.5 Protección del sistema

La protección de la red comienza inmediatamente después de la instalación. Un sistema que cubra muchas necesidades, antes de pasar al régimen de explotación debe ser muy seguro, ya que es una herramienta de la que depende el trabajo de muchas personas.

La seguridad ocupa gran parte del tiempo y esfuerzo de los administradores. Lo habitual es que antes de hacer una instalación de red, el administrador ya haya pensado en su seguridad.

Hay que establecer unos mecanismos de seguridad contra los distintos riesgos que pudieran atacar al sistema de red. Analizaremos aquí los riesgos más comunes.

A. Protección eléctrica

Todos los dispositivos electrónicos de una red necesitan corriente eléctrica para su funcionamiento. Los ordenadores son dispositivos especialmente sensibles a perturbaciones en la corriente eléctrica. Cualquier estación de trabajo puede sufrir estas perturbaciones y perjudicar al usuario conectado en ese momento en la estación. Sin embargo, si el problema se produce en un servidor, el daño es mucho mayor, ya que está en juego el trabajo de toda o gran parte de una organización. Por tanto, los servidores deberán estar especialmente protegidos de la problemática generada por fallos en el suministro del fluido eléctrico.

Algunos factores eléctricos que influyen en el funcionamiento del sistema de red son los siguientes:

- **Potencia eléctrica en cada nodo,** especialmente en los servidores, que son los que soportan más dispositivos, por ejemplo, discos. A un servidor que posea una fuente de alimentación de 200 vatios no le podemos conectar discos y tarjetas que superen este consumo, o incluso que estén en el límite. Hay que guardar un cierto margen de seguridad si no queremos que cualquier pequeña fluctuación de corriente afecte al sistema. Los grandes servidores corporativos suelen tener fuentes de alimentación de mayor potencia con objeto de poder alimentar más hardware y, además, redundantes para evitar problemas en caso de fallos en la fuente.

- **La corriente eléctrica debe ser estable.** Si la instalación eléctrica es defectuosa, deberemos instalar unos estabilizadores de corriente que aseguren los parámetros básicos de la entrada de corriente en las fuentes de alimentación de los equipos. Por ejemplo, garantizando tensiones de 220 voltios y 50 Hz de frecuencia. El estabilizador evita los picos de corriente, especialmente los producidos en los arranques de la maquinaria.

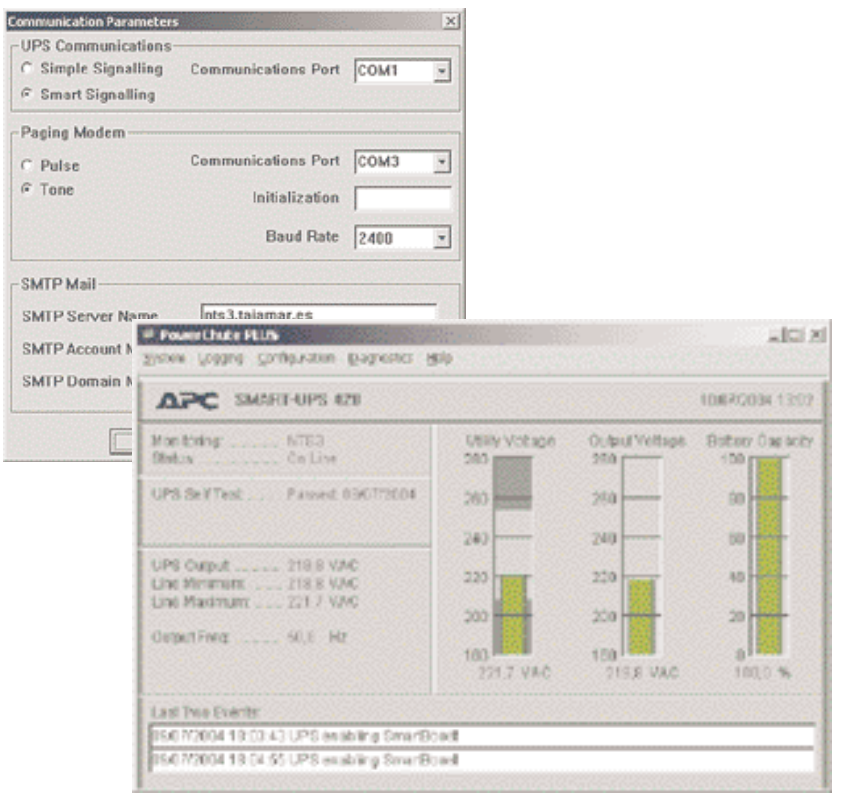

Figura 7.14. *Parámetros configurables en una estación para el gobierno de un SAI.*

- **Correcta distribución del fluido eléctrico y equilibrio entre las fases de corriente.** En primer lugar, no podemos conectar a un enchufe de corriente más equipos de los que puede soportar. Encadenar ladrones de corriente en cascada no es una buena solución. Además, las tomas de tierra (referencia común en toda comunicación) deben ser lo mejores posibles.

  Si la instalación es mediana o grande, deben instalarse picas de tierra en varios lugares y asegurarse de que todas las tierras de la instalación tienen valores similares. Una toma de tierra defectuosa es una gran fuente de problemas intermitentes para toda la red, además de un importante riesgo para los equipos.

- **Garantizar la continuidad de la corriente.** Esto se consigue con un **SAI** (Sistema de Alimentación Ininterrumpida) o UPS.

Normalmente, los sistemas de alimentación ininterrumpida corrigen todas las deficiencias de la corriente eléctrica: actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etcétera.

El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que permite cerrar el sistema de red adecuadamente, guardar los datos que tuvieran abiertos las aplicaciones de los usuarios y cerrar ordenadamente los sistemas operativos.

Si además no queremos vernos obligados a parar nuestra actividad, hay que instalar grupos electrógenos u otros generadores de corriente conectados a nuestra red eléctrica. Básicamente hay dos tipos de SAI:

- **SAI de modo directo.** La corriente eléctrica alimenta al SAI y éste suministra energía constantemente al ordenador. Estos dispositivos realizan también la función de estabilización de corriente.

- **SAI de modo reserva.** La corriente se suministra al ordenador directamente. El SAI sólo actúa en caso de corte de corriente.

Los servidores pueden comunicarse con un SAI a través de alguno de sus puertos de comunicaciones, de modo que el SAI informa al servidor de las incidencias que observa en la corriente eléctrica.

En la Figura 7.14 se pueden observar algunos de los parámetros que se pueden configurar en un ordenador para el gobierno del SAI.

Windows, por ejemplo, lleva ya preconfigurada una lista de SAI de los principales fabricantes con objeto de facilitar lo más posible la utilización de estos útiles dispositivos.

B. Protección contra virus

Los virus informáticos son programas o segmentos de código maligno que se extienden (infección) por los ficheros, memoria y discos de los ordenadores produciendo efectos no deseables y, en ocasiones, altamente dañinos.

Algunas empresas de software, especializadas en seguridad, han creado programas (antivirus) que detectan y limpian las infecciones virulentas.

Si ya es importante que una estación de trabajo aislada no se infecte con virus, mucho más importante es evitar las infecciones en un servidor o en cualquier puesto de red, ya que al ser nodos de intercambio de datos, propagarían extraordinariamente la infección por todos los puestos de la red.

Es posible la instalación de aplicaciones antivirus en los servidores, corriendo en ***background***, que analizan cualquier fichero que se deposita en el servidor.

Esto ralentiza el servidor, puesto que consume parte de los recursos de procesamiento, pero eleva la seguridad.

El auge de Internet y las aplicaciones instaladas en ella o que se pueden descargar desde servidores web ha provocado una explosión de virus transmitidos a su través: los virus más comunes en la actualidad se transmiten dentro de los mismos mensajes de correo electrónico.

Las compañías fabricantes de software antivirus han tenido que idear utilidades antivíricas que chequean estos correos electrónicos y vigilar intensivamente cualquier software que entre por las líneas de conexión a Internet.

Los más modernos antivirus pueden llegar a centralizar sus operaciones sobre una consola que vigila atentamente toda la red (Figura 7.15).

Corresponde al administrador advertir de estos riesgos a los usuarios de la red, limitar los accesos a las aplicaciones y a los datos que puedan portar virus e impedir la entrada de datos indeseados, por ejemplo, a través de disquetes, CD-ROM o Internet.

Debe planificar las copias de seguridad con la debida frecuencia para restituir el sistema en caso de desastre.

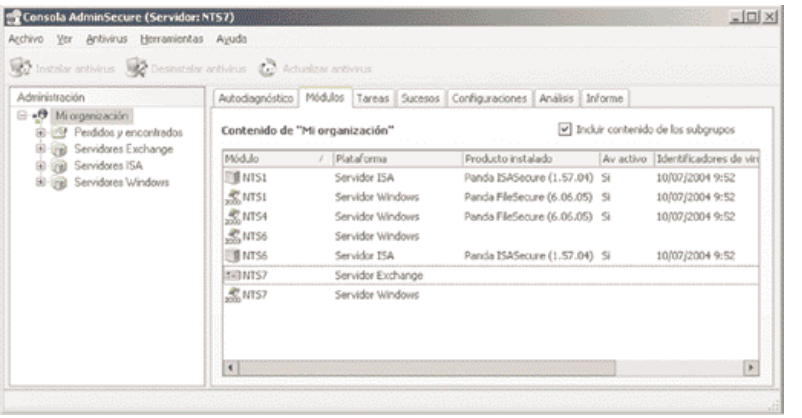

Figura 7.15. *Consola de administración centralizada para toda una red de un conocido antivirus sobre Windows.*

Actividad

4 Instala una aplicación antivirus que puedes descargar de Internet en una estación cliente. Verifica la limpieza del sistema en que se ha instalado.

Seguidamente, descarga de Internet la versión de servidor de un antivirus y prueba a hacer una instalación en red. Para realizar esto deberás seguir las instrucciones del fabricante.

Desde la consola de administración, ensaya la instalación del antivirus de cliente desde un punto central hasta el resto de las estaciones de la red.

C. Protección contra accesos indebidos

Además de las cuentas personalizadas de usuario, los NOS disponen de herramientas para limitar, impedir o frustrar conexiones indebidas a los recursos de la red.

Para ello, se pueden realizar auditorías de los recursos y llevar un registro de los accesos a cada uno de ellos.

Si un usuario utilizara algún recurso al que no tiene derecho, seríamos capaces de detectarlo o, al menos, de registrar el evento.

Conviene realizar un plan de auditorías en que se diseñen los sucesos que serán auditados. Las auditorías se pueden realizar sobre conexiones, accesos, utilización de dispositivos de impresión, uso de ficheros o aplicaciones concretas, etcétera. El auditor genera un registro de accesos que puede ser consultado por el administrador de red en cualquier momento.

Además, es posible definir el disparo de alarmas que avisen de que ciertos eventos han ocurrido en la red, utilizando el sistema de mensajería electrónica del NOS (Figura 7.16).

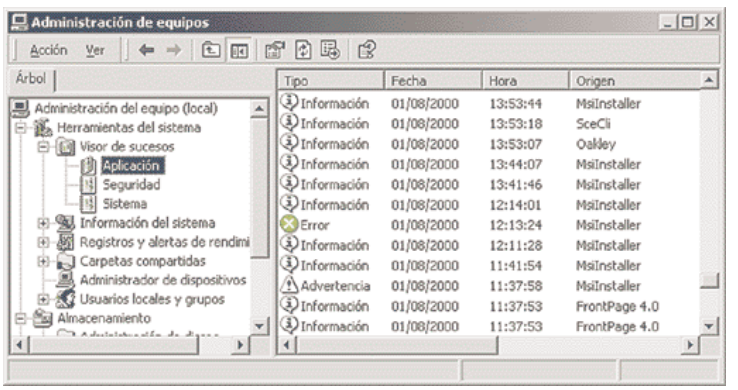

Figura 7.16. *Visor de sucesos de Windows.*

También es posible visualizar el estado de las conexiones y accesos al servidor: observar la corrección de su utilización, detener conexiones, estadísticas de utilización, etcétera.

Cada conexión al servidor consume recursos del servidor, normalmente CPU y memoria. Por tanto, es aconsejable limitar el número máximo de conexiones que se permitirán en cada recurso, teniendo en cuenta las necesidades de los usuarios y el rendimiento del sistema.

Hay programas cuyo propósito es la captura del nombre y la contraseña de los usuarios de la red o hacerse con información privilegiada para su posterior uso ilegal. Estos programas pertenecen al grupo de los denominados **caballos de Troya.** Los sistemas deben estar protegidos contra estos programas.

Ante la abundancia de redes de organizaciones que se conectan a otras redes WAN, se deben instalar unos dispositivos denominados **cortafuegos,** que limitan los accesos de usuarios externos a la propia LAN. En la Unidad 9 se estudiarán con mayor profundidad estos dispositivos de red.

Actividad

5 Define en un sistema un conjunto de alertas y auditorías que dejen un rastro claro de la actividad del sistema o de los accesos de los usuarios. Deja el sistema funcionando durante un tiempo provocando accesos no autorizados y vuelve más tarde a observar los ficheros de registro de actividad. Extrae las conclusiones pertinentes y propón soluciones contra los accesos indebidos.

D. Protección de los datos

El software más importante en las estaciones de trabajo de cualquier organización está representado por los datos de usuario, ya que cualquier aplicación puede ser reinstalada de nuevo en caso de problemas; los datos, no.

La duplicación de los datos

El modo más seguro de proteger los datos ante cualquier tipo de problemas es duplicarlos. Se puede tener un doble sistema de almacenamiento en disco, pero esto genera nuevos problemas, entre los que destacamos:

- Cuando se tiene información duplicada es difícil determinar cuál de las copias es la correcta.
- La duplicación de información requiere la inversión de más recursos económicos, al ocupar más espacio en los dispositivos de almacenamiento.

Copias de seguridad

La **copia de seguridad** o ***backup*** es una duplicación controlada de los datos o aplicaciones de los usuarios. Se realiza a través de utilidades propias de los sistemas operativos y del hardware apropiado.

Cabe la posibilidad de que las unidades de backup estén centralizadas en los servidores, de modo que con pocas unidades se puedan realizar las copias de todo el sistema. El software de las utilidades de backup puede automatizarse para que las copias se realicen automáticamente en periodos apropiados, por ejemplo, por la noche, salvando los datos que hayan sido modificados durante el día. Los medios físicos más comunes para realizar este tipo de volcado son la cinta magnética y el CD o DVD regrabables. La relación capacidad/coste es mayor que en el caso de discos duplicados. Las desventajas residen en que la lectura de los datos de un backup no es directa por las aplicaciones y requieren un volcado inverso (de cinta a disco) previo.

Ejemplos de cintas utilizadas para backup son las DLT, QIC, DAT, *streamers*, etc. Algunas de ellas pueden alcanzar una gran capacidad utilizando sofisticadas técnicas de compresión de datos, por encima de los 100 Gbytes. En la operación de *backup* también se pueden utilizar discos, normalmente removibles, e incluso CD o DVD grabables. En cualquier caso, siempre hay que exigir que el dispositivo de *backup* tenga capacidad para almacenar los datos que haya que guardar, lo que normalmente exigirá que el sistema pueda generar múltiples volúmenes en un único *backup*.

Se pueden establecer distintos tipos de copias de seguridad, destacamos aquí dos de ellas:

- ***Backup* normal.** Es una copia de los archivos seleccionados sin ninguna restricción, posiblemente directorios completos y sus subdirectorios.

- ***Backup* progresivo, diferencial o incremental.** En este caso, la copia sólo se realiza sobre los ficheros seleccionados que hayan sido modificados o creados después del anterior backup.

Las copias de seguridad realizadas sobre cualquier sistema deben estar perfectamente etiquetadas y documentadas con el fin de garantizar que la recuperación de ficheros, en caso de problemas, sea de la copia correcta (Figura 7.17).

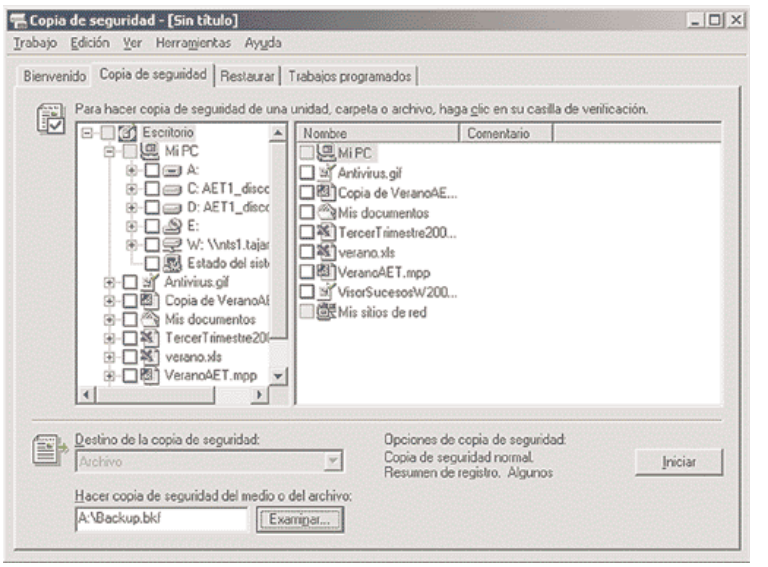

Figura 7.17. *Utilidad para la copia de seguridad en Windows.*

Sistemas tolerantes a errores

Un sistema tolerante a errores es aquél que está capacitado para seguir operando aunque se presenten fallos en alguno de sus componentes.

La tolerancia a fallos está diseñada para combatir fallos en periféricos, en el software de sistema operativo, en la alimentación eléctrica de los equipos, etcétera.

La tolerancia a fallos más común es la que consiste en duplicar los elementos del sistema, por ejemplo, que cada equipo posea dos fuentes de alimentación: cuando falla una de ellas, automáticamente se pone en funcionamiento la segunda.

En el caso de discos, el método de redundancia más sencillo es la configuración de discos espejo *(mirror)*. Para ello, se duplican los discos, de modo que cualquier operación de escritura sobre uno de los discos se duplica en el otro.

En la lectura, cualquier disco puede proporcionar los datos solicitados, puesto que son iguales.

Los sistemas operativos de red avanzados poseen software para la automatización de los procesos de tolerancia a errores.

En los sistemas actuales se proporcionan un conjunto de tecnologías que, en conjunto, contribuyen a crear sistemas seguros, escalables y de alta disponibilidad. La exigencia de muchos sistemas es 24 x 7, es decir, 24 horas diarias y 7 días por semana.

Se considera que un sistema es seguro si tiene una disponibilidad superior al 99,99 %, es decir, un día de paro de sistema por cada 10 000 de utilización.

Actividad

6 Establece un directorio de datos como objetivo de un backup. Realiza una copia de seguridad del mismo. Ahora elimina el directorio copiado y restaura la información comprobando que la información restaurada es idéntica a la que se salvó.

Ahora, según vas cambiando algunos datos del directorio objetivo, ve haciendo backups incrementales. Finalmente, restaura todos los backups y comprueba que la información restaurada es la correcta.

Genera un automatismo para que se haga un backup del sistema a cierta hora y comprueba que a la hora prevista se dispara el backup.

Tecnología RAID

La tecnología más extendida para la duplicación de discos es la RAID (*Redundant Array of Inexpensive Disks*, serie redundante de discos económicos), que ofrece una serie de niveles de seguridad o crecimiento de prestaciones catalogados de 0 a 5, aunque algunos no se utilizan:

- **RAID de nivel 0.** Los datos se reparten entre varios discos mejorando las prestaciones del acceso a disco, aunque no se ofrece ningún tipo de redundancia.

- **RAID de nivel 1.** La redundancia de datos se obtiene almacenando copias exactas cada dos discos, es decir, es el sistema de espejos al que nos hemos referido anteriormente.

- **RAID de nivel 2.** No ha sido implementado comercialmente, pero se basa en la redundancia conseguida con múltiples discos una vez que los datos se han dividido en el nivel de bit.

- **RAID de nivel 3.** Los datos se dividen en el nivel de byte. En una unidad separada se almacena la información de paridad.

- **RAID de nivel 4.** Es similar al nivel 3, pero dividiendo los datos en bloques.

- **RAID de nivel 5.** Los datos se dividen en bloques repartiéndose la información de paridad de modo rotativo entre todos los discos.

Por ejemplo, Windows NT, Windows 2000 y Windows 2003 soportan RAID 1 y RAID 5 en cualquiera de sus versiones servidoras. Microsoft denomina **espejos** o ***mirrors*** a RAID 1 y **sistemas de bandas con paridad** a RAID 5. En la Figura 7.18 hay un ejemplo de gestor de discos con RAID 1 en un sistema servidor Windows.

Para establecer discos espejo (RAID 1) sólo son necesarios dos discos, mientras que para la utilización de las bandas con paridad, el mínimo de discos es de tres.

Todas las operaciones de gestión de discos se realizan desde el administrador de discos que se halla integrado en la consola de administración local del equipo en el caso de Windows (Figura 7.18).

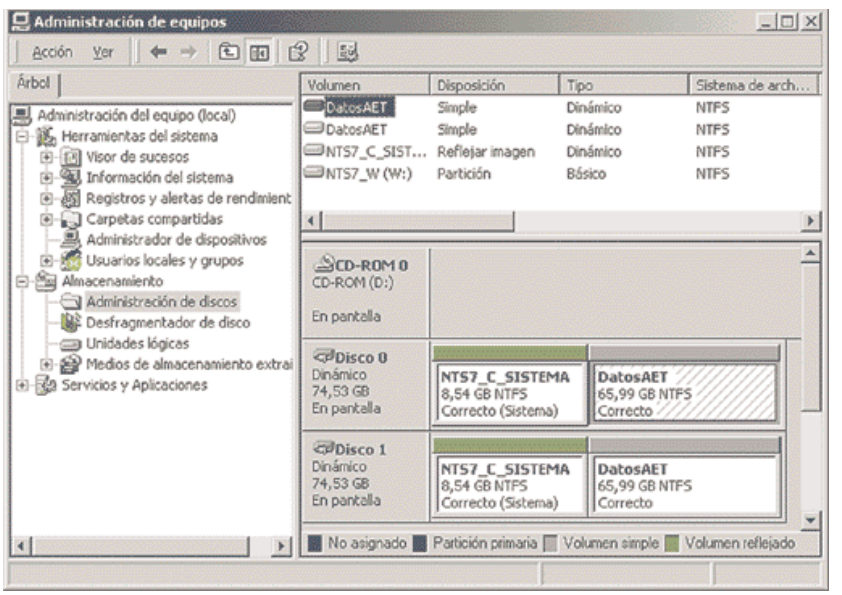

Figura 7.18. *Gestor de discos en Windows Server con un volumen RAID 1.*

Actividad

7 Sobre un servidor Windows (no funcionaría sobre una versión cliente), instala dos discos duros, en uno de los cuales instalarás el sistema operativo.

Una vez instalado, comprueba que el sistema ve los dos discos físicos desde el administrador de discos de Windows. Ahora convierte en dinámicos los dos discos. Crea un espejo del disco de sistema en el segundo disco. Una vez terminada la operación, comprueba que puedes arrancar un sistema idéntico desde cualquiera de los dos discos.

Posteriormente, estando el sistema en funcionamiento con el espejo correctamente realizado, apaga abruptamente el equipo desconectando la alimentación. Vuelve a encender el equipo, preséntate en él y arranca el administrador de discos.

Observarás que el espejo se está reconstruyendo para garantizar la integridad de la información en los dos discos: el apagón no permitió la sincronización de datos y ahora el sistema pone en marcha mecanismos de reparación.

Dispositivos extraíbles en caliente

Llegar a estos niveles de disponibilidad en los sistemas no es nada sencillo; los ordenadores no son más que máquinas electrónicas y, por tanto, están expuestos a todo tipo de catástrofes.

Algunas compañías han diseñado componentes de ordenadores que son intercambiables en caliente, es decir, sin apagar el ordenador.

Esta característica está muy extendida en los discos duros de un cierto nivel. De hecho, en general, los discos en configuración RAID suelen residir en torres de discos conectadas al procesador central o a la red a través de buses de comunicaciones muy rápidos, y suelen ser intercambiables en caliente.

Últimamente, en servidores muy especializados, están apareciendo tarjetas que también se pueden cambiar en caliente.

El desarrollo de las técnicas *Plug & Play* en los sistemas operativos, por ejemplo en Windows, hace que el sistema reconozca inmediatamente la nueva tarjeta y prosiga su funcionamiento en pocos segundos.

Configuraciones en cluster

Para una instalación, disponer de un único servidor es un gran riesgo: el trabajo de una empresa se puede paralizar si su servidor corporativo falla. Los *clusters* de servidores vienen a solucionar, entre otros, este problema.

Un **cluster** es una asociación de ordenadores que comparten periféricos de almacenamiento y entre los que se establecen unas fuertes relaciones de cooperación en el trabajo que realizan.

Así, si uno de los servidores del cluster deja de funcionar, otro miembro de ese cluster absorberá su trabajo. El rendimiento del sistema se resentirá de algún modo (se ha perdido un servidor), pero no se perderá la funcionalidad total del sistema.

Entre los sistemas operativos de red capaces de organizarse en forma de clusters están algunas versiones de UNIX, Windows NT Advanced Sever, Windows 2000 Advanced Server y Datacenter Server, y las versiones superiores de Windows 2003 Server.

Plan de contingencias ante desastres

Aunque se pongan todas las medidas imaginables, siempre puede darse una situación no prevista en la que el sistema deje de funcionar.

El tiempo de parada será menor si está previsto (e incluso probado) con antelación cómo hacer frente a cada avería concreta.

El documento que recoge qué hacer en cada momento se denomina **plan de contingencias.** Es uno de los documentos más importantes que debe preparar el administrador de red.

El plan de contingencias es la mayor garantía de que no se dejará llevar por la precipitación ante una situación de desastre.

E. La seguridad en la red

Teniendo en cuenta que muchas redes se conectan a Internet a través de dispositivos que las ocultan, la cifra de ordenadores que pueden volcar datos a Internet es gigantesca.

Lo que a nosotros nos interesa ahora es que la inseguridad de nuestro sistema puede venir, entre otros factores, por cualquiera de esos nodos de la red.

Pretendemos aquí dar, a modo de ejemplo, unos cuantos consejos tomados de publicaciones del sector que se deben tener en cuenta cuando se planifica la seguridad de la red de una corporación:

- La seguridad y la complejidad suelen guardar una relación de proporcionalidad inversa, es decir, a mayor seguridad, se simplifican los procedimientos, ya que la seguridad es limitadora de las posibilidades.
- Además, la educación de los usuarios de la red debe ser lo más intensa posible.
- La seguridad y la facilidad de uso suelen guardar frecuentemente una relación de proporcionalidad inversa; por tanto, resulta conveniente concentrarse en reducir el riesgo, pero sin desperdiciar recursos intentando eliminarlo por completo, lo que es imposible.
- Un buen nivel de seguridad ahora es mejor que un nivel perfecto de seguridad nunca.
- Por ejemplo, se pueden detectar diez acciones por hacer; si de ellas lleva a cabo cuatro, el sistema será más seguro que si se espera a poder resolver las diez.
- Es mejor conocer los propios puntos débiles y evitar riesgos imposibles de cuantificar.
- La seguridad es tan potente como su punto más débil, por lo que interesa centrarse en estos últimos puntos.
- Lo mejor es concentrase en amenazas probables y conocidas.
- La seguridad no es un gasto para la empresa, sino que debe ser considerada como una inversión.

Al plantearse el diseño de la seguridad de la red a la luz de los consejos anteriores, hay que seguir una serie de pasos, entre los que destacan los siguientes:

- Evaluar los riesgos que corremos.
- Definir la política fundamental de seguridad de la red.
- Elegir el diseño de las tácticas de seguridad.
- Tener previstos unos procedimientos de incidencias-respuesta, etcétera.

7.6 Control remoto en la red

Cuando una instalación de red es de tamaño reducido o no se extiende mucho en su ámbito geográfico, el administrador de red puede desplazarse con facilidad por las distintas estaciones y servidores para realizar su función profesional sobre ellos.

Sin embargo, cuando no se cumplen estos requisitos, son necesarias herramientas especializadas en la gestión remota de los ordenadores y dispositivos de la red. La mayor parte de estas herramientas son capaces de saltar la barrera impuesta por la redes de área local, proporcionando sus beneficios también a través de redes de área extensa. El objetivo básico de cualquiera de estas herramientas es reducir al máximo posible el coste total de propiedad (TCO, *Total Cost of Ownership*) de los equipos, facilitando el retorno de la inversión (ROI, *Return Of Investment*).

Fundamentalmente, hay dos modelos de gestores remotos: los que se encargan de la gestión de equipos y los que tienen por función la gestión de consolas. El número de elementos en una red que se puede gestionar es tan grande que es imposible abarcarlo todo, proponemos como ejemplo la iniciativa WfM (*Wired for Management*, conectado para la gestión) de Intel, o la interfaz WMI de Microsoft.

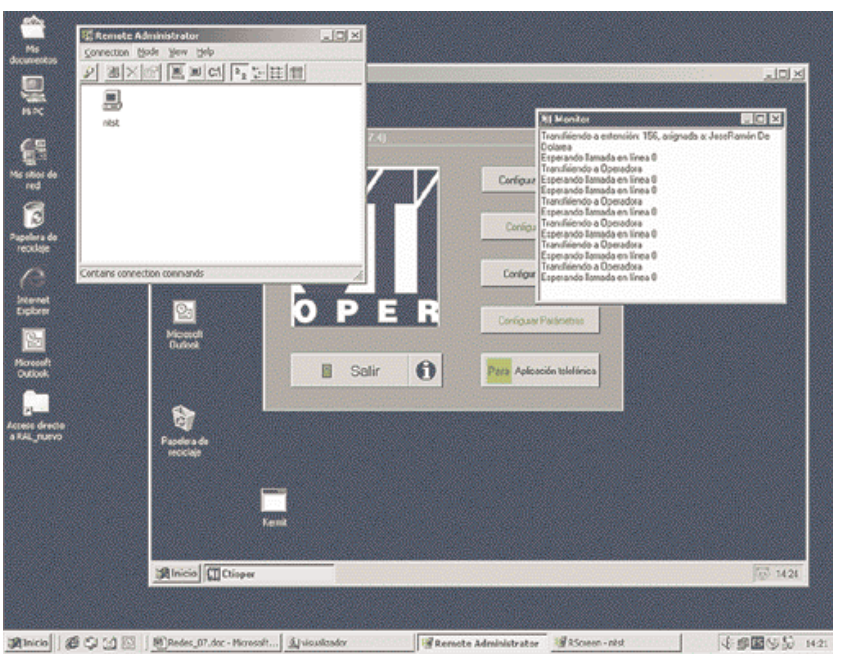

Figura 7.19. *Conexión remota desde Windows 2000 con destino en otro sistema Windows con Remote Administrator, un gestor de conexiones comercial.*

A. El gestor de equipos e instalaciones

Un gestor de instalaciones es un conjunto de herramientas integradas entre sí y con el sistema operativo sobre el que se instala que es capaz de llevar un control exhaustivo sobre el software de cada sistema, así como de su configuración y funcionamiento.

En muchos casos, este software es capaz de controlar también los escritorios y accesos de los usuarios que se presentan en cada estación de la red. Cada fabricante de software incorpora unas funciones a sus productos de gestión; sin embargo, las funciones básicas más comunes de un gestor de equipos son las siguientes:

- **Despliegue de sistemas y de software.** El gestor es capaz de instalar sistemas operativos y software adicional desde los servidores de gestión en los que se apoya de acuerdo con la parametrización que diseña el administrador de sistemas.

- **Configuración de los equipos.** Una vez instalados los equipos, el gestor es capaz de proporcionar las configuraciones básicas de cada equipo o de cada usuario; por ejemplo, el administrador del sistema podría definir las aplicaciones a las que se tienen acceso, los recursos que serán visibles para cada usuario, etcétera.

- **Control de equipos y de la red.** El gestor puede analizar cada una de las incidencias ocurridas en los equipos de la red y tomar las acciones previstas por el administrador de red en cada uno de los eventos.

Con Windows 2000 Server y versiones superiores, Microsoft ha dado un gran paso adelante, integrando en su sistema herramientas avanzadas de instalación, todo ello controlado a través de una política de directivas integradas en su Directorio Activo, aunque su herramienta de gestión por excelencia para grandes redes es SMS *(Server Management System)*.

B. El gestor de consolas

Un gestor de consolas o simplemente gestor de control remoto es una aplicación que es capaz de visualizar sobre una consola local lo que está ocurriendo en una consola remota. Los más avanzados son capaces también de crear verdaderas sesiones remotas, no sólo simularlas.

Además, los gestores más avanzados son capaces de ejecutar acciones en el sistema remoto comandados desde el sistema local.

Un gestor remoto ofrece grandes ayudas; sin embargo, las funciones más beneficiadas son las siguientes:

- **Administración de red.** Desde un único punto geográfico pueden controlar todos los servidores y estaciones de la red: crear, modificar o eliminar usuarios o grupos, instalar o configurar aplicaciones, reiniciar ordenadores, etcétera.

- **Teletrabajadores.** Cualquier persona desde el exterior de la red podrá conectarse y acceder a su información de red.

- **Soporte, asistencia técnica y mantenimiento.** Estas funciones constituyen uno de los mayores ámbitos comerciales para este tipo de aplicaciones, pues se pueden brindar todos estos servicios remotamente sin necesidad de costosos desplazamientos.

- **Formación.** La tecnología utilizada por un gestor de consolas es muy apropiada para su configuración en forma de aula virtual, en el seno de la cual se pueda impartir formación. Para ello, es necesario que el gestor permita que varias sesiones locales puedan conectarse a una única sesión remota.

El transporte de red necesitado por estos gestores para mover datos a través de la red utiliza los protocolos básicos que ya hemos estudiado: TCP/IP, IPX/SPX, etcétera.

Destacamos la solución VNC por ser *freeware* y de amplio uso (se puede descargar desde www.realvnc.com) y, además, por estar soportada por muchos UNIX, Linux, Windows en todas sus variantes, OS/2, BeOS, MacOS, PalmOS y muchos más sistemas operativos.

Microsoft con Windows NT propuso un modelo de creación de sesiones remotas desde estaciones de la red con su versión *Terminal Edition*. Windows 2000 ha recogido esta tecnología y permite que una estación de trabajo se conecte a un servidor Windows 2000 como si fuera un cliente ligero.

Se permiten hasta dos conexiones con objeto de hacer administración remota sin necesidad de licencia adicional. El cliente puede ser cualquiera de las versiones Windows de Microsoft, incluida Windows 3.11.

En la Figura 7.20 se puede ver el asistente de conexión y la consola local una vez realizada la conexión remota.

En Windows XP y Windows 2003 Server también se pueden crear conexiones remotas a través de la gestión remota del escritorio.

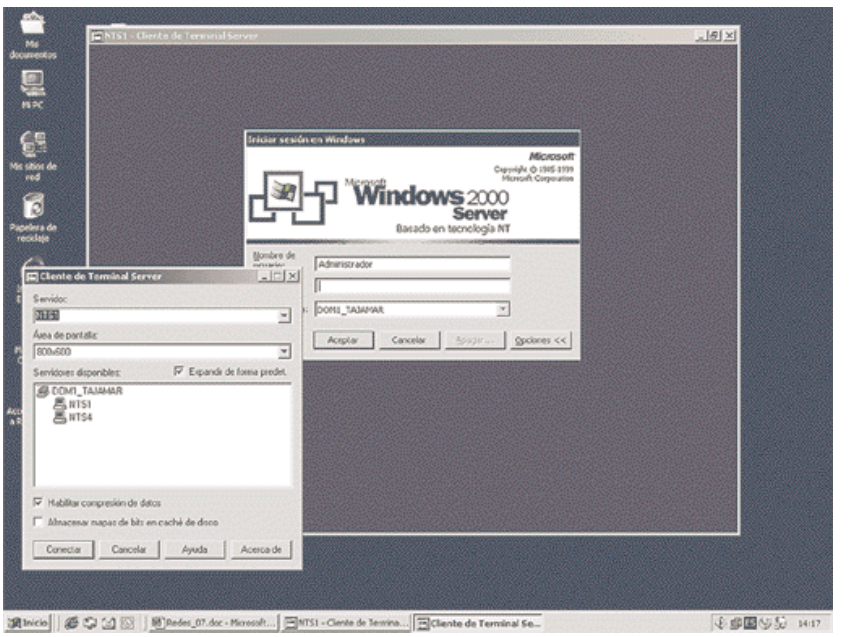

Figura 7.20. *Asistente de conexión y conexión realizada desde una estación Windows a un servidor Windows.*

Actividad

8 Descarga de Internet la aplicación gratuita VNC. Esta aplicación consta de un cliente (visualizador) y un servidor, que se instala como un servicio automático del sistema operativo.

Instálala en dos nodos de la red con el mismo sistema operativo y configúralos para que puedan hacerse conexiones cruzadas.

Comprueba que puedes hacer conexiones remotas.

Ahora instala VNC en otro nodo de la red con sistema operativo distinto, incluso Linux o MacOS X (existen versiones de VNC también para estos sistemas operativos). Prueba su funcionalidad.

C. Iniciativa WfM de Intel

WfM (*Wired for Management*, conectado para la gestión) es una iniciativa de Intel para establecer un estándar con algunas de las propiedades de la gestión remota de las estaciones de red.

WfM se apoya sobre otros estándares ya establecidos, pero su gestión se centra en cuatro niveles:

- Gestión previa al inicio del sistema.
- Gestión del consumo energético.
- Gestión de la información.
- Agentes de soporte.

La gestión previa al inicio de WfM está enfocada a la gestión de estaciones de trabajo cuando éstas están apagadas. La tecnología **PXE** (*Previous eXecution Environment*, entorno de ejecución previo al inicio), especificación para la gestión en adaptadores de red, es obligatoria bajo WfM: tanto la BIOS del PC como la tarjeta de red deben soportarlo.

Actividad

9 Instala un equipo Windows en red que tenga una tarjeta de red compatible con la tecnología PXE y con esta funcionalidad habilitada. Deja esta estación apagada pero conectada a la corriente eléctrica. La placa madre de este sistema tiene que contemplar también la posibilidad de arranque del sistema por red.

Busca en Internet una aplicación *Wake on LAN* que sea capaz de despertar al equipo. Instala en el mismo segmento de red otra estación en la que se ejecutará la aplicación. Ejecútala pasándole como argumento la dirección física de la tarjeta PXE y comprueba que la estación se enciende automáticamente.

Con la tecnología PXE la tarjeta de red permanece siempre a la escucha de la red, aún con el PC apagado, de modo que a una orden concreta del servidor, la tarjeta ordena encenderse al PC arrancando el software de sistema: una tecnología denominada **WOL** (*Wake On LAN*).

Pero un PC que pueda despertarse también tiene que ser capaz de autoapagarse; por eso, WfM integra la tecnología **ACPI** (*Advanced Configuration Power Interface*, Interfaz de consumo energético y configuración avanzada) en las BIOS, que es capaz de realizar estas operaciones.

También se necesita un entorno de gestión de información. WfM se adapta a cualquier entorno de gestión que hayamos cargado con el software de red: agentes SNMP, DMI o CIM.

WOL despierta a un equipo cuando recibe por la tarjeta de red, que permanece siempre a la escucha aun con el equipo apagado (que no desconectado de la red eléctrica), una trama específica denominada **trama mágica** desde un gestor de arranque.

Como esta característica opera en el nivel de enlace (capa 2 de OSI), el encendido sólo funcionará dentro del mismo segmento de la red de área local. Si se quieren despertar máquinas remotas, hay que utilizar mecanismos de enrutamiento junto con WOL.

7.7 Autenticación y certificación

El avance de la etapa comercial en el desarrollo de Internet y la integración de la venta electrónica de productos o transacciones financieras electrónicas ha generado unas expectativas en el volumen de negocio en las que el principal problema reside en la seguridad. Analizaremos en este epígrafe los conceptos básicos utilizados en Internet, y por extensión en el resto de las redes, sobre tecnologías y protocolos de seguridad.

A. La criptografía

Encriptar un mensaje no es más que codificarlo de nuevo de acuerdo con un código que sólo el destinatario de la información conoce, haciendo por tanto ilegible el mensaje al resto de los posibles receptores. En Internet, es típico codificar la información económica sensible, como los datos de la tarjeta de crédito. Entre las funciones básicas del cifrado podemos citar las siguientes:

- **Confidencialidad.** Los datos sólo deben ser legibles por los destinatarios autorizados.
- **Integridad.** Los datos deben ser genuinos. El sistema debe detectar si los datos originales han sido cambiados.
- **Autenticación.** Se trata de asegurarse de que la información fue originada por quien se dice en el mensaje. Más adelante estudiaremos este asunto con más profundidad.

El principal problema de la criptografía es cómo custodiar la información de codificación, ya que quien la posea será capaz de restituir el mensaje original, perdiéndose, por tanto, su privacidad. Muchos algoritmos de encriptación utilizan una clave que modifica particularmente el comportamiento del algoritmo, de modo que sólo quien conozca esa clave podrá desencriptar el mensaje.

Se pueden utilizar muchos algoritmos para encriptar mensajes:

- **DES, *Data Encription Standard*.** Es el sistema de encriptación oficial americano. Emplea un algoritmo con clave secreta de 56 bits, lo que significa que oculta la clave entre más de 72 000 billones de posibles combinaciones. Para hacernos una idea, un algoritmo de este tipo utilizado habitualmente en Internet utiliza una clave de 1 024 bits.

- **RSA, *Rivest, Shamir, Adleman*.** Este algoritmo lleva por nombre las iniciales de los apellidos de sus creadores, investigadores del MIT *(Massachussets Institute of Technology)* y que crearon este algoritmo en 1997. Se basa en dos claves, una pública y otra privada, que son complementarias entre sí, pero que no son deducibles una a partir de la otra. El mensaje encriptado con una clave pública sólo puede ser desencriptado con la clave privada complementaria y viceversa. RSA es el pionero en la tecnología **PKI** *(Public Key Infrastructure)*.

Por la importancia que reviste el algoritmo RSA, merece la pena dedicarle algo más de atención. Veamos brevemente cómo funciona el algoritmo. Cuando un emisor quiere enviar un mensaje a un receptor, el emisor encripta el mensaje utilizando la clave pública (de todos conocida) del receptor. El receptor es el único que conoce y posee su propia clave privada. El mensaje encriptado sólo puede ser desencriptado por quien conozca la clave privada del receptor, es decir, sólo podrá ser leído por el receptor a quien el emisor designó. Por tanto, cualquier persona puede enviar mensajes encriptados a cualquier receptor, ya que las claves públicas son eso, públicas. Sin embargo, sólo un receptor, el que posea la clave privada del destinatario del mensaje, podrá leerlo.

No son estos los únicos sistemas de encriptación utilizados en Internet; basta con pasearse por las opciones o preferencias de cualquier navegador de Internet para observar la inclusión dentro del navegador de muchos otros algoritmos.

B. Certificados digitales

El certificado digital es una credencial que proporciona una Autoridad de Certificación que confirma la identidad del poseedor del certificado, es decir, garantiza que es quien dice ser.

La Autoridad de Certificación actúa de modo semejante a un notario digital y es quien expide los certificados electrónicos que se guardan en los ordenadores de los usuarios, normalmente accesibles desde su navegador de Internet. El ámbito de utilización de las firmas electrónicas es muy amplio; aquí destacamos algunas aplicaciones más comunes:

- **Justificación ante las administraciones.** La firma electrónica sirve como documento de identidad electrónico y válido, por ejemplo, se pueden pagar los impuestos a través de Internet con seguridad.

- **Comercio electrónico.** Con la firma digital se puede evitar que los compradores repudien operaciones de compra realmente realizadas o bien asegurarse de que el web de comercio electrónico es auténtico: no es la suplantación de un tercero.

- **Transacciones financieras.** Un ejemplo claro es el de los monederos electrónicos seguros. La firma digital puede ir asociada al monedero garantizando la transacción.

- **Software legal.** Cualquier software instalado en un equipo debe ir correctamente firmado como garantía del fabricante.

- **Correo electrónico.** Con la firma digital se asegura la autenticación del remitente del mensaje.

Formalmente, un certificado digital es un documento electrónico emitido por una entidad de certificación autorizada para una persona física o jurídica, con el fin de almacenar la información y las claves necesarias para prevenir la suplantación de su identidad. Dependiendo de la política de certificación propuesta por la Autoridad de Certificación, cambiarán los requisitos para la obtención de un certificado, llegándose incluso al caso de tener que presentarse físicamente el interesado para acreditar su identidad.

Por ejemplo, la ACE (Agencia de Certificación Electrónica en España) emite tres tipos de certificados: el de clase 1 no exige contrastar ninguna información especial, basta con el nombre del usuario y una dirección de correo a donde se le enviará el certificado. Para la clase 2, el usuario debe presentar documentación que acredite su identidad, pero no requiere su presencia. Sin embargo, para los de clase 3 sí se requiere la presencia física del usuario que solicita el certificado. Este certificado ACE de clase 3 es equivalente en cuanto a seguridad a los de clase 2 emitidos por la Fábrica Nacional de Moneda y Timbre en España para la Agencia Tributaria.

El certificado está protegido por un identificador que sólo conoce el propietario del mismo, aunque es posible su almacenamiento en dispositivos más seguros como tarjetas inteligentes *(smartcards)* o llaves USB.

C. Autenticación

Cuando el usuario de una red se presenta en su sistema, lo que realmente está haciendo es informando a la red de quién es para que el sistema le proporcione los derechos, permisos y recursos que tenga asignados personalmente. ¿Cómo sabe la red que el usuario que se intenta presentar es quien dice ser? Éste es el problema que resuelven los sistemas de autenticación.

El certificado digital proporciona un mecanismo seguro para producir una correcta autenticación, ya que la Autoridad de Certificación asegura la veracidad de la información. En los sistemas de red, los certificados digitales residen en un servicio de directorio al que accede el sistema para contrastar la información procedente de la Autoridad de Certificación.

Windows Server y muchas versiones de UNIX son ejemplos típicos de este sistema de autenticación. El sistema operativo lleva incorporado un generador y servidor de certificados para ser utilizados internamente en la red si no se desean utilizar los servicios de una compañía certificadora externa a la red. Kerberos es la tecnología de autenticación mediante firma electrónica más extendida actualmente.

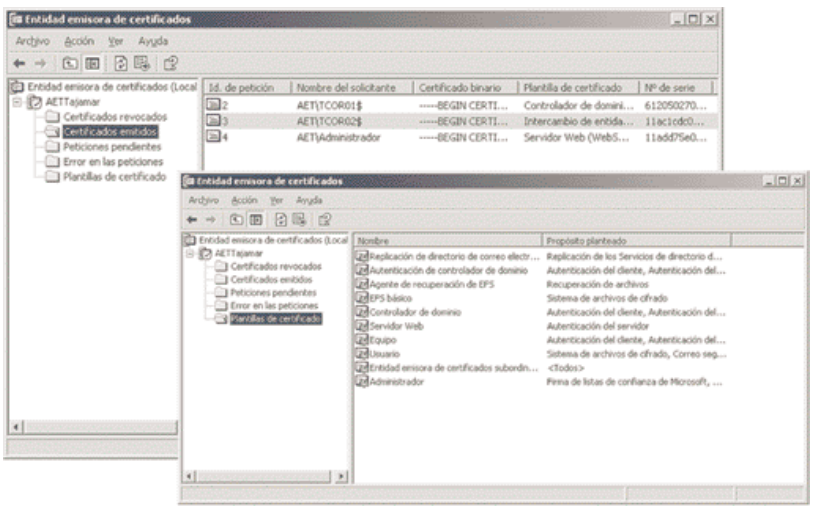

Figura 7.21. *Consola de administración de una entidad emisora de certificados integrante de una PKI en Windows Server 2003.*

D. Componentes de una PKI

Una **PKI** (*Public Key Infrastructure*, infraestructura de clave pública) es un conjunto de elementos de infraestructura necesarios para la gestión de forma segura de todos los componentes de una o varias Autoridades de Certificación.

Por tanto, una PKI incluye los elementos de red, servidores, aplicaciones, etc. Ahora vamos a identificar algunos de los componentes lógicos básicos de una infraestructura de clave pública.

- **Autoridad de certificación CA.** Una autoridad de certificación es el componente responsable de establecer las identidades y de crear los certificados que forman una asociación entre la identidad y una pareja de claves pública y privada.

- **Autoridad de registro RA.** Una autoridad de registro es la responsable del registro y la autenticación inicial de los usuarios a quienes se les expedirá un certificado posteriormente si cumplen todos los requisitos.

- **Servidor de certificados.** Es el componente encargado de expedir los certificados aprobados por la autoridad de registro. La clave pública generada para el usuario se combina con otros datos de identificación y todo ello se firma digitalmente con la clave privada de la autoridad de certificación.

- **Repositorio de certificados.** Es el componente encargado de hacer disponibles las claves públicas de las identidades registradas antes de que puedan utilizar sus certificados. Suelen ser repositorios X.500 o LDAP. Cuando el usuario necesita validar un certificado debe consultar el repositorio de certificados para verificar la firma del firmante del certificado, garantizar la vigencia del certificado comprobando su periodo de validez y que no ha sido revocado por la CA y que además cumple con los requisitos para los que se expidió el certificado; por ejemplo, que el certificado sirve para firmar correo electrónico.

Los sistemas operativos avanzados como Windows Server suelen incorporar software suficiente para construir una infraestructura de clave pública completa (Figura 7.21).

En el cifrado de la información pueden emplearse muchos métodos, pero fundamentalmente se utilizan dos: sistemas de una sola clave y sistemas de dos claves, una privada y otra pública.

En el caso de utilizar una única clave, tanto el emisor como el receptor deben compartir esa única clave, pues es necesaria para desencriptar la información.

Hasta aquí no hay ningún problema; sin embargo, el procedimiento de envío de esta clave al receptor que debe descifrar el mensaje puede ser atacado permitiendo que un intruso se apodere de esa clave.

Mucho más seguros son los procedimientos de doble clave. Consisten en confeccionar un par de claves complementarias, una de las cuales será pública, y que por tanto puede transmitirse libremente, y otra privada que sólo debe estar en posesión del propietario del certificado y que no necesitará viajar. El algoritmo hace que un mensaje cifrado con la clave pública sólo pueda descifrarse con la clave privada que le complementa y viceversa.

Cuando el emisor quiere enviar un mensaje a un receptor, cifra la información con su clave privada que sólo él posee. El receptor, una vez que le haya llegado el mensaje cifrado, procederá a descifrarlo con la clave pública del emisor (Figura 7.22).

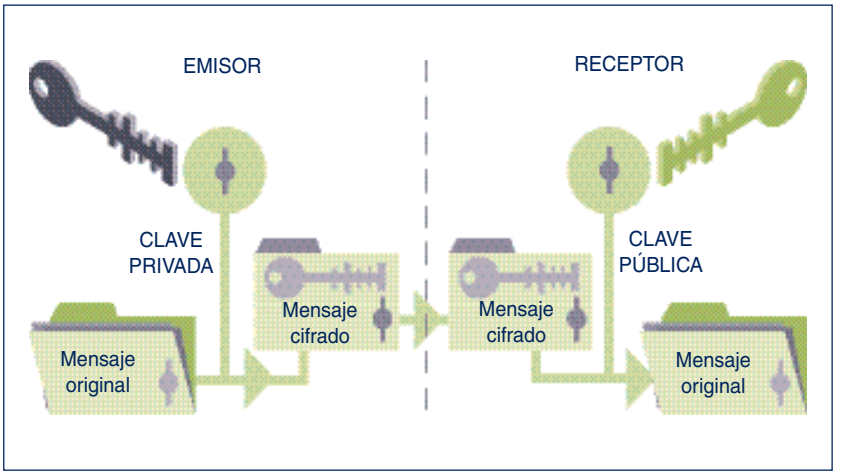

Figura 7.22. *Cifrado y descifrado utilizando algoritmos de parejas de claves: pública y privada.*

E. Firma electrónica

La firma electrónica sirve para garantizar la integridad de un mensaje firmado, es decir, asegura que la información no fue manipulada por el camino. La firma normalmente es un resumen del propio mensaje firmado. Este resumen se obtiene mediante algoritmos de resumen y cifrado como SHA-1 o MD5, que comprimen el mensaje de forma que el receptor, aplicando el mismo algoritmo al mensaje recibido, debe obtener un resumen idéntico al que ha recibido adjuntado al mensaje por el emisor y que ha obtenido por el mismo procedimiento. Cualquier manipulación del mensaje generaría en el destino un resumen distinto del elaborado por el emisor, y se detectaría así la intrusión.

Actividad

10 Sobre un servidor Windows instala los servicios de certificación. Crea una oficina de certificación siguiendo la documentación que proporciona el fabricante con el sistema. Ahora ensaya distintas soluciones para generar certificados digitales.

Genera un certificado para un servidor web concreto. Descarga el certificado e instálalo en el servidor web a través de la ficha correspondiente del IIS. Habilita la conexión al servidor web a través de SSL y prueba que puedes acceder a alguna página de ese servidor desde el explorador a través del protocolo HTTPS.

F. Protocolos seguros

Haremos aquí una descripción de los protocolos y tecnologías que se utilizan en la actualidad para dotar a los sistemas en red de mecanismos de comunicación seguros.

Protocolo SSL

Desde hace algunos años, el protocolo más utilizado para encriptar comunicaciones por Internet es **SSL** *(Secure Sockets Layer)*, desarrollado por Netscape. Se trata de un protocolo que encripta una comunicación punto a punto seleccionando un método de encriptación y generando las claves necesarias para toda la sesión. En la arquitectura de red se sitúa inmediatamente por encima de la capa de transporte; por ejemplo, en una transmisión de páginas web seguras desde un servidor web hasta un navegador, SSL estaría entre la capa del protocolo http y la capa de transporte propia de TCP o UDP.

Aunque las claves generadas por SSL son débiles, es difícil romperlas en el tiempo que dura una transacción, por lo que, sin ser el mejor protocolo de seguridad, es muy válido. SSL es uno de los protocolos más utilizados en la creación de redes privadas virtuales (VPN, *Virtual Private Networks*).

SSL, sin embargo, no resuelve el problema de la autenticación. Además, el receptor de la información puede acceder a toda la información, lo que en el caso del comercio electrónico es un problema: el vendedor no sólo tendría acceso al pedido (datos a los que tiene derecho), sino también la información bancaria del comprador, datos que son propios de las entidades bancarias.

Cuando desde el navegador se pretende realizar una compra por Internet, SSL suele activarse en el momento de realizar el pago, de modo que la información de la tarjeta de crédito viaja encriptada. Esta activación se produce en la web del comerciante utilizando el protocolo https, una variante de http que incorpora las técnicas de encriptación.

Veamos algo más detenidamente cómo funciona SSL desde un navegador de Internet a través de las fases que atraviesa:

a) En la primera fase, el navegador solicita una página a un servidor seguro. La petición queda identificada por el protocolo https en vez de http, utilizado en páginas no seguras. A continuación, navegador y servidor negocian las capacidades de seguridad que utilizarán a partir de ese momento.

b) Seguidamente, se ponen de acuerdo en los algoritmos que garanticen la confidencialidad, integridad y autenticidad.

c) En una tercera fase, el servidor envía al navegador su certificado de norma X.509 que contiene su clave pública y, si la aplicación lo requiere, solicita a su vez el certificado del cliente.

d) A continuación, el navegador envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos que se hayan de intercambiar como seguros. El envío de esta clave se hace cifrándola con la clave pública del servidor que extrajo previamente de su certificado.

e) Finalmente, se comprueba la autenticidad de las partes implicadas y, si el canal ha sido establecido con seguridad, comenzarán las transferencias de datos.

Los certificados X.509 se utilizan para garantizar que una clave pública pertenece realmente a quien se atribuye. Son documentos firmados digitalmente por una autoridad de certificación, que asegura que los datos son ciertos tras demostrárselo el solicitante del certificado documentalmente.

Contienen la clave pública los datos que identifican al propietario, los datos de la autoridad de certificación y la firma digital generada al encriptar con la clave privada de la autoridad de certificación.

SSL aporta muchas ventajas a las comunicaciones seguras. En primer lugar, goza de gran popularidad y se encuentra ampliamente extendido en Internet, además de estar soportado por la mayor parte de los navegadores actuales.

También asegura cualquier comunicación punto a punto, no necesariamente de transmisión de páginas web, aunque ésta es la aplicación de mayor uso. Por último, el usuario no necesita realizar ninguna operación especial para activar el protocolo: basta con sustituir en el navegador la secuencia http por https.

SET

Los problemas de SSL están solucionados en **SET** (*Secure Electronic Transaction*, Transacción electrónica segura). En 1995, Visa y MasterCard, ayudados por otras compañías como Microsoft, IBM, Netscape, RSA o VeriSign, desarrollaron SET ante el retraimiento tanto de las compañías comerciantes como de los posibles compradores hacia el comercio electrónico o financiero.

SET es muy complicado, así que resumiremos aquí brevemente su funcionamiento. Cuando A quiere efectuar una compra en B, genera un pedido para B y decide el medio de pago. Entonces B genera un identificador de proceso para la compra y lo envía a A con su clave pública y la de una pasarela de pago C que se utilizará en la transacción. El comprador envía a B dos informaciones: la primera es el pedido, que estará encriptado con la clave pública de B, de manera que sólo el vendedor pueda leer el pedido.

La segunda información es el modo de pago, que A encriptará con la clave pública de la pasarela de pagos C. De este modo, aunque la información sea recibida inicialmente por B, sólo C podrá leer los datos bancarios. El banco, sin embargo, no puede leer el pedido realizado, que sólo puede ser desencriptado por B, su destinatario; por tanto, el banco no puede realizar un estudio del perfil del comprador.

A partir de aquí, la pasarela de pagos C consultará con los bancos emisor y receptor de la transacción para que se autorice. Si se cumplen todos los requisitos, se produce la transacción, informando al vendedor y comprador de que la operación de compra-venta ha sido realizada correctamente.

Protocolos seguros para correo y el acceso a redes

Además de SSL y SET existen otros protocolos que ayudan a mantener comunicaciones seguras. Las técnicas criptográficas no dejan de avanzar porque de las garantías de seguridad en las comunicaciones depende en gran medida el avance en el comercio electrónico, las oficinas electrónicas de la administración pública, etcétera.

Encriptación PGP

PGP son las siglas de *Pretty Good Privacy*. Se trata de un sistema de encriptación gratuito de cualquier tipo de información, aunque se ha extendido sobre todo por su capacidad de cifrar mensajes de correo electrónico basado en el modelo de firma digital, de modo que se garantiza la autenticación del remitente.

Está ampliamente extendido en la comunidad Internet y se integra en la mayoría de los clientes de correo electrónico. También se puede encontrar como una suite de aplicaciones separadas.

Es posible descargar el software necesario para gran parte de los sistemas operativos de muchos servidores en Internet de la dirección www.pgpi. com/download.

Protocolo PPTP

PPTP son las siglas de *Point to Point Tunneling Protocol* o protocolo de túnel punto a punto. Es un protocolo definido en el RFC 2637 que pretende mantener un servicio punto a punto cifrado protegiendo la comunicación del exterior.

Frecuentemente, PPTP se combina con otros protocolos como L2TP, que estudiaremos más adelante.

PPTP es bastante popular en redes privadas virtuales, ya que Microsoft incorporó un servidor y un cliente PPTP gratuitos a partir de Windows NT. En la Unidad 9 hablaremos más extensamente de VPN y PPTP.

Protocolo IPSec

Se trata de un conjunto de extensiones del TCP/IP que añade autenticación y encriptación en la transmisión de paquetes.

IPSec consta de tres elementos diferenciados: cabeceras de autenticación, bloques de seguridad y un protocolo de negociación e intercambio de claves. Con estos elementos se pueden producir fenómenos de transporte tradicionales o bien en forma de túneles, seguros en cualquiera de los casos. Microsoft incorpora IPSec a partir de Windows 2000. En la Unidad 9 también nos extenderemos en este protocolo.

Actividad

11 Siguiendo la información proporcionada por la web oficial de PGP, instala un sistema de encriptación PGP y prueba su funcionamiento.

Prueba a enviar mensajes de correo electrónico cifrados con PGP de manera que los destinatarios de los mensajes, provistos también con esta tecnología, puedan descifrarlos.

7.8 Optimización de la red

Una vez instalada la red, y en pleno funcionamiento, se debe pasar al periodo de observación y medida con el fin de asegurarnos que se obtiene el mayor rendimiento posible.

Esta tarea se compone de una fase de análisis de la red con la elaboración de unas estadísticas sencillas que sirvan de apoyo para la proposición de medidas correctoras en los cuellos de botella que se produzcan o en la incorporación de mejoras.

En el mercado, existen paquetes de software capaces de hacer estos análisis de red, aunque siempre exigen la decisión globalizadora del responsable de la red.

A. Análisis de problemas y medidas correctoras

Los parámetros en los que hay que detenerse a la hora de analizar una red varían de unas redes a otras; sin embargo aquí expondremos los más comunes.

Una vez detectado el problema se propondrán diversos tipos de soluciones posibles.

Rendimiento de la CPU de los servidores

Los servidores de red son máquinas altamente consumidoras de recursos de procesamiento. Si el servidor tiene que brindar muchos servicios distintos o a muchos usuarios, es posible que el cuello de botella se sitúe en la velocidad de proceso de la CPU, ralentizando todo el trabajo de la red (Figura 7.23).

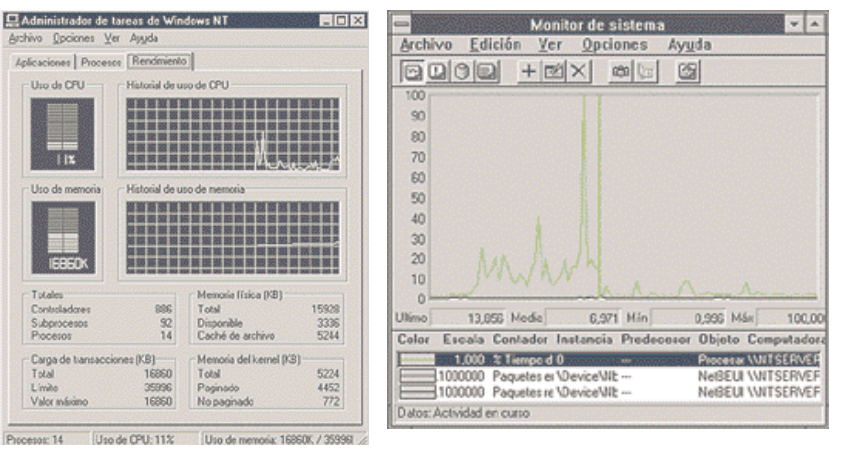

Figura 7.23. *Ejemplos de monitorización de algunos parámetros en un servidor Windows.*

El bajo rendimiento se manifiesta notablemente cuando el servidor no es capaz de suministrar información a los dispositivos de impresión que tiene conectados en los puertos o si tiene que gestionar entradas/salidas en tiempo real.

Éste es el caso, por ejemplo, de la recepción o envío de datos a través del módem que tiene conectado por un puerto serie.

Las soluciones a este problema de escalabilidad se pueden enfocar desde distintos puntos de vista:

- **Sustitución del procesador por otro más rápido.** Esto no siempre es posible, puesto que los procesadores más modernos llevan diferentes encapsulados y patillajes de conexión a la placa madre.

- Además, no todas las placas son compatibles con todos los procesadores, aunque el zócalo del procesador sí sea compatible. Por ejemplo, no todas las placas soportan las mismas velocidades de reloj.

- **Incorporar más procesadores al servidor.** Si el hardware y el software lo permiten, esta solución mejora sensiblemente el problema, especialmente si los buses de comunicaciones de los procesadores con memoria son rápidos. En la actualidad, muchos servidores incorporan ya de serie más de un procesador.

- **Incrementar el número de servidores.** Esta solución fracciona la red de modo que se reparte la carga entre todos los servidores. En su aspecto más avanzado, se puede llegar a una configuración de proceso distribuido, transparente al usuario, con lo que se consiguen buenos equilibrios de carga.

Algunas de las soluciones comentadas requieren sistemas operativos escalables como UNIX, o sistemas Windows a partir de su versión 2000. En general, interesa que las CPU de servidores sean procesadores aventajados de 32 o 64 bits, que incorporen características avanzadas con el fin de obtener altos rendimientos. Además, conviene que estén construidas de acuerdo con arquitecturas escalares, es decir, que permitan el crecimiento de la tecnología en el sistema y que permitan que el mismo software pueda correr en procesadores de distintas prestaciones.

Paginación

Cuando un servidor está escaso de memoria central genera un cuello de botella en el sistema de paginación. Los sistemas operativos utilizados en la actualidad necesitan una gran cantidad de recursos de memoria para ejecutar las aplicaciones.

Como la memoria central es un bien escaso en cualquier equipo informático, el sistema se las ingenia volcando a disco (memoria virtual paginada) los datos residentes en memoria que prevé no utilizar de momento. El proceso de intercambio de datos entre memoria y disco recibe el nombre de **paginación.**

El tiempo de acceso medio a memoria central es de unas decenas de nanosegundos, mientras que el de acceso a disco es de una decena de milisegundos. Por tanto, si un sistema pagina demasiado, se ralentizarán todas las operaciones. Si el nivel de paginación es elevado, interesa incorporar más memoria central al sistema. Es bastante común obtener fuertes incrementos en el rendimiento del sistema sin más que ampliar su memoria RAM, ya que decrecerá el nivel de paginación.

Niveles de transferencia de entrada y de salida

A veces, el cuello de botella se sitúa en los discos: demasiados usuarios realizando operaciones de entrada o salida de los discos, la paginación del sistema, el disparo de aplicaciones remotas desde el servidor, etcétera.

Aunque el sistema disponga de una CPU muy rápida y de grandes cantidades de memoria, si hay demasiadas operaciones de entrada y salida de los discos, la CPU estará casi siempre en estado de espera y el rendimiento decaerá notablemente.

En estos casos se pueden tomar las siguientes medidas de mejora:

- **Mejorar el rendimiento de los controladores de disco o del bus de comunicaciones.** Por ejemplo, si tenemos un bus IDE, se podría incorporar un bus SCSI de alta velocidad o tecnologías de Fibre Channel.

  Además los controladores disponen de varios modos de funcionamiento, de manera que podremos seleccionar aquél que más convenga al tipo de discos de que dispongamos.

- **Incrementar el número de discos.** Al tener un mayor número de discos, la carga de entrada y salida se repartirá entre todos ellos, mejorando el rendimiento global del sistema.

- **Repartir los accesos a discos entre varios volúmenes,** que pertenezcan a distintos discos o incluso a distintos sistemas.

Tráfico de red

Como ya hemos estudiado, algunas redes como Token Ring gestionan perfectamente las situaciones de tráfico intenso en la red. Sin embargo, otras como Ethernet se comportan mal cuando están sobrecargadas.

Esto hace importante la observación periódica del tráfico de red, así como de los parámetros por los que se regula; por ejemplo, en Ethernet, se podría medir el nivel de colisiones habidas frente al volumen de datos transferidos con éxito.

En el mercado existen aplicaciones que analizan el tráfico de red. A veces, incluso vienen incorporadas con el propio sistema operativo de red (Figura 7.24).

Los parámetros que suelen analizar son muy variados y dependen del tipo de protocolo utilizado y del tipo de red, así como de la topología de la misma.

Algunos analizadores de red tienen mecanismos que generan tráfico controlado para observar la respuesta de la red en situaciones concretas a través de un proceso de simulación de situaciones reales.

Posibles soluciones de mejora para estos problemas podrían ser la asignación de máscaras de red más ajustadas a las necesidades de la propia red, modificaciones en la topología de red, concentrar los nodos que generan mucho tráfico en segmentos de red rápidos, asegurarse de que se cumplen las especificaciones de los fabricantes en cuanto a longitudes de cables y parámetros eléctricos, etc.

También es posible segmentar la red con la utilización de switches y encaminadores.

Si el tráfico de red es muy intenso, no habrá más remedio que dar un salto tecnológico en la composición de la red.

Por ejemplo, la evolución natural de una red Ethernet es pasar a Fast Ethernet y de ésta a Gigabit Ethernet. También se pueden construir segmentos de fibra óptica o configurar la red con ATM, tecnología que será estudiada en la Unidad 8.

Monitorización de los protocolos de red

La mayor parte de los analizadores de red son capaces de elaborar estadísticas sobre el tipo de tráfico que observan en la red, determinando qué tramas han sido generadas por cada protocolo que convive en la red.

Esto es especialmente importante cuando los paquetes generados por algunos protocolos deben ser transportados a otra red a través de encaminadores, ya que estas máquinas trabajan con paquetes de protocolos previamente seleccionados. Estos dispositivos serán estudiados con profundidad en la Unidad 9.

Cuando se dan situaciones de este tipo, es necesario observar frecuentemente el estado de puentes, encaminadores y pasarelas, puesto que un cuello de botella en alguno de estos elementos puede perjudicar la marcha global de la red, aunque en ella no haya un tráfico intenso.

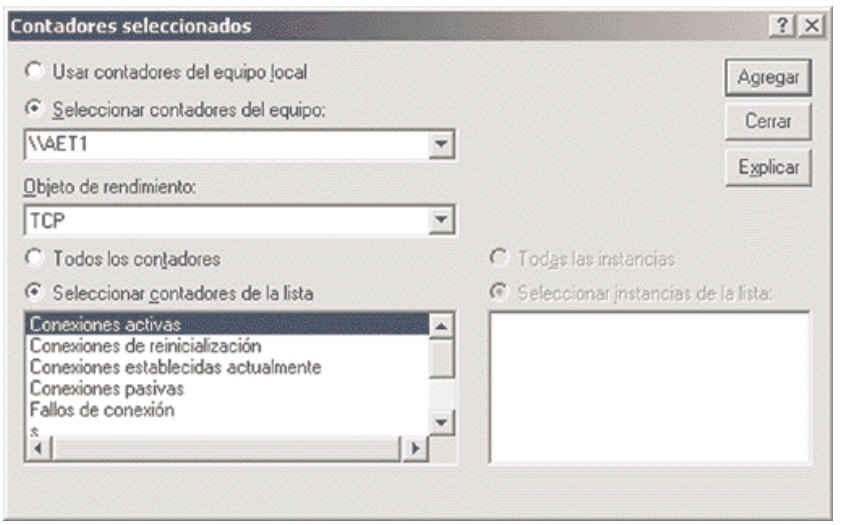

Figura 7.24. *Parametrización de un analizador de red básico incorporado en Windows y accesible desde el administrador de sistema.*

B. Protocolos para la gestión de redes

El crecimiento experimentado por las redes de área local y, sobre todo, la aparición de sistemas distribuidos, ha generado la aparición de técnicas y protocolos especializados en la gestión de redes.

La idea de partida es conseguir que desde un único puesto de la red (el del administrador) denominado **consola,** se pueda monitorizar toda la red.

Estas tecnologías recogen información de cada uno de los nodos, observando el tráfico en cada uno de los segmentos de la red, avisando en el caso de que se llegue a situaciones que el administrador de la red defina como alarmantes.

En muchos sistemas también se permite la reconfiguración de la red y la simulación de situaciones comprometidas para la red.

Los dispositivos gestionados en una red disponen de un agente que envía alarmas si detecta problemas o situaciones anómalas en la red.

Por otra parte, se instalan en la red otros programas denominados entidades de gestión, que recogen e interpretan estas alarmas disparando los mecanismos oportunos para informar al administrador de red o corregir los problemas.

Además, las entidades de gestión interrogan periódicamente a los agentes de red sobre su estado. De este modo, la entidad de gestión se hace una composición de lugar sobre el estado de la red en cada instante.

Este sistema de pregunta/respuesta *(polling)* se realiza mediante protocolos especializados como SNMP (*Simple Network Management Protocol*, protocolo básico de gestión de red).

La información recogida se almacena en una base de datos denominada MIB (*Management Information Base*, base de datos de información de gestión).

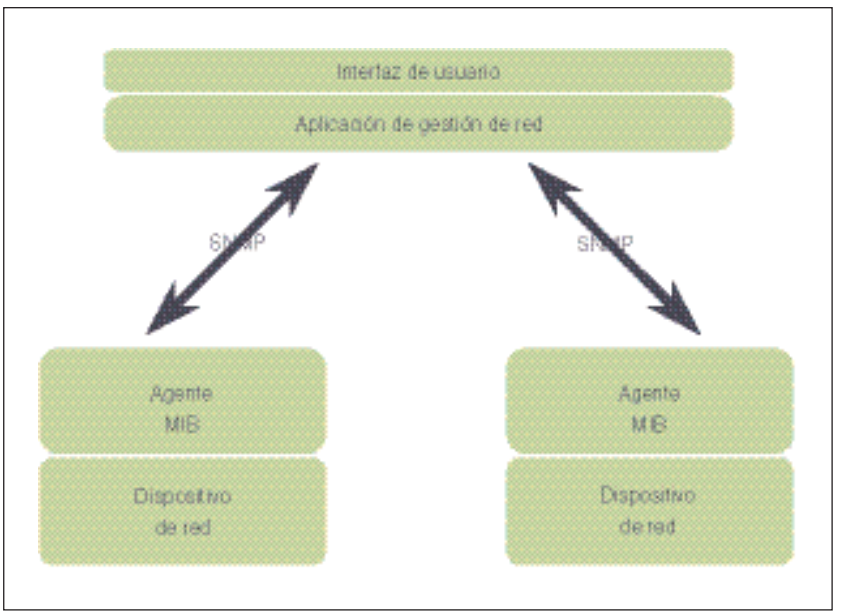

Figura 7.25. *Arquitectura de la gestión de red con SNMP.*

A partir de los MIB (Figura 7.25), las aplicaciones de gestión elaboran estadísticas y otros informes que permiten al administrador tomar decisiones estratégicas sobre la funcionalidad y la seguridad de la red en cada uno de sus puntos.

La ISO ha sugerido cinco áreas de control para las aplicaciones de gestión de redes, aunque después los productos comerciales de los distintos fabricantes añaden otros parámetros.

Los parámetros sugeridos por la ISO son los siguientes:

- Rendimiento de la red.
- Configuración de los dispositivos de red.
- Tarifa y contabilidad de los costes de comunicaciones en la red.
- Control de fallos.
- Seguridad de la red.

SNMP es un protocolo de gestión de redes que recoge y registra información desde los dispositivos de una red que siguen su estándar a través de un sistema de preguntas y respuestas.

Esta información es almacenada en un gestor centralizado desde donde se procesará.

Pero SNMP tiene algunos problemas. En primer lugar no es demasiado escalable, es decir, el crecimiento de la red hace que se genere mucho tráfico si se quiere hacer una buena gestión.

En segundo lugar, no permite la monitorización de muchos segmentos, lo que lo hace inapropiado para grandes redes.

RMON (*Remote MONitoring*, monitorización remota) es un sistema de gestión de red que viene a resolver en parte estos problemas del SNMP.

RMON provee entre otras las siguientes informaciones en su MIB, llamado **MIB2** y definido en la RFC 1213:

- Estadísticas. Tráfico de red y errores, así como estadísticas en el nivel de tramas MAC.
- Historia, recogida a intervalos periódicos para su posterior análisis.
- Alarmas y eventos. Definiendo un umbral por encima del cual se disparan.
- Conversaciones entre dos dispositivos cualesquiera.
- Filtrado de paquetes.

RMON sólo es capaz de monitorizar un segmento de red en el nivel de direcciones MAC, lo que frecuentemente es una limitación importante.

Un progreso se produce en la iniciativa RMON2 de la IETF (RFC 2021), que da el salto hasta el nivel 3 de OSI, atacando la gestión de la red a través de direcciones IP.

Sin embargo, la solución aún no es completa. La solución más avanzada es la utilización de **SMON** (*Switched MONitoring*, monitorización conmutada), definida en la RFC 2613, que con su nuevo MIB es capaz de gestionar los dispositivos de red y las redes privadas virtuales, no sólo los puertos de comunicaciones, como ocurría en el caso de RMON.

La mayor parte de los sistemas operativos de red ponen los protocolos adecuados para realizar una gestión de red.

Son escasos los sistemas que proporcionan una consola de análisis de lo que está ocurriendo en la red; normalmente, este software suele ser suministrado por terceras compañías (véase Figura 7.26).

Empieza a ser habitual que la gestión de dispositivos de red se realice a través del navegador de Internet.

Bastantes dispositivos que se conectan a la red incorporan, además de su funcionalidad propia, un pequeño servidor web que sirve para configurarlo y administrarlo.

En la actualidad, los protocolos de gestión de red se encuentran en plena evolución. Los estándares de facto en evolución más importantes son los siguientes:

- **SNMPv2** (versión 2 del SNMP).
- **RMON.**
- **DMI** (*Desktop Management Interface*, interfaz de gestión de escritorio), propuesto por el DMTF (*Desktop Management Task Force*, grupo de trabajo de gestión de escritorio).
- **CMIP**, que es la solución OSI.

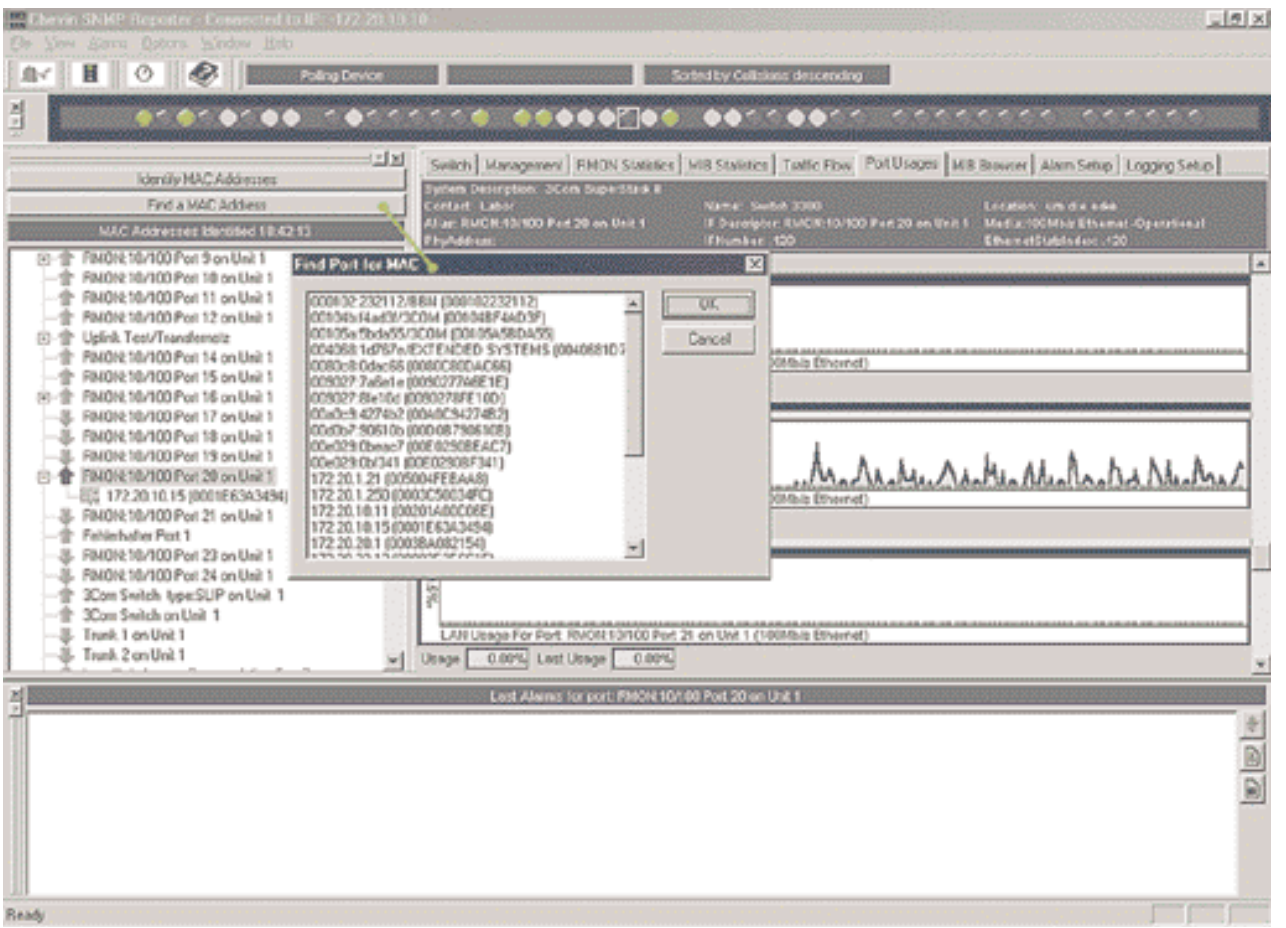

Figura 7.26. *Ejemplo de aplicación que gestiona tanto SNMP como RMON.*

7.9 Documentación del sistema

Ante la posibilidad de cualquier problema, cambio o mejora en la red, es conveniente tener documentado correctamente el sistema con la información lo más actualizada posible.

Cada administrador de red elige las técnicas de documentación que considera oportunas. No obstante, los documentos que no pueden faltar son los siguientes:

- **Mapa de red.** Es la representación gráfica de la topología de la red, incluyendo tanto conexiones internas como externas. Esta documentación puede apoyarse en un plano del edificio en donde se instala la red.

  Suelen confeccionarse dos tipos de mapas de red: *lógicos* y *físicos*. En los **lógicos** o funcionales, se indica la funcionalidad del elemento que se describe, así como sus direcciones, función que desempeña, etc. En el caso del mapa **físico,** interesa sobre todo la especificación de la conectividad del cableado.

- **Mapa de nodos.** Se compone de una descripción del hardware y del software que se instala en cada nodo, así como los parámetros de su configuración, modelos, marcas, direcciones de red, etc. La documentación debe permitir la creación de un histórico de cada nodo que registre la evolución de sus averías, actualizaciones de software, etcétera.

- **Mapa de protocolos.** Es la descripción de la organización lógica de la red, así como de los protocolos utilizados globalmente, por ejemplo, las direcciones de máscaras de red, configuración de las pasarelas y de los encaminadores, zonas AppleTalk, creación de dominios o grupos de trabajo, relaciones de confianza, etcétera.

- **Mapa de grupos y usuarios.** Consiste en la descripción de los grupos y usuarios de la red contemplando las posibilidades de acceso a los distintos recursos, así como los derechos de acceso a las aplicaciones, perfiles, privilegios, etcétera.

- **Mapa de recursos y servicios.** Muestra todos los recursos disponibles identificando sus nombres, el servicio que prestan, el lugar físico o lógico en que residen y los usuarios o grupos a los que se les permite el acceso, el servicio de directorio en el que quedarán publicados, etcétera.

- **Calendario de averías.** Es el registro de averías del sistema, de modo que permita el análisis de las causas y probabilidad de fallo de los distintos componentes de la red, tanto software como hardware, y su evolución en el tiempo.

- **Informe de costes.** Es el estudio económico tanto del mantenimiento como de las nuevas inversiones del sistema.

- **Plan de contingencias.** Ya hemos comentado anteriormente la importancia de este documento, que es la base de actuación ante cualquier desastre.

Actividad

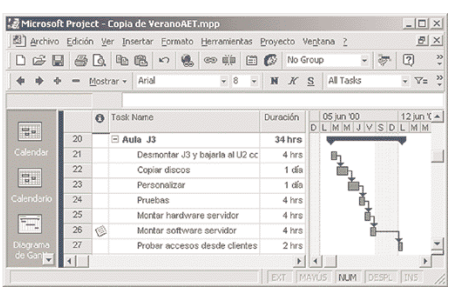

Figura 7.27. *Ejemplo de diagrama de Gantt para el control de un proyecto de instalación.*

12 Toma una solución de instalación de red (real o ficticia) y genera toda la documentación de red posible.

Para la realización de esta documentación puedes ayudarte de las herramientas típicas de una suite ofimática.

Puedes generar documentos de texto, gráficos de instalación, plantillas para rellenar averías y sus soluciones, diagramas de Gantt (véase Figura 7.27) para ajustar los tiempo de las distintas fases de proyectos, etcétera.

7.10 Casos de estudio para el diseño de redes

Seguidamente, presentamos dos casos en donde se sugiere una posible solución dentro del ámbito de las redes de área local sobre necesidades reales de dos organizaciones. Obviamente, la solución no es única. Está abierta a muchas otras posibilidades. La solución que aquí se ofrece es orientativa.

En la Unidad 9 se ofrecerán nuevos casos para el diseño de redes corporativas que además utilizan redes de área extendida.

Por el momento, nos centraremos en las necesidades de una pequeña organización y de una de tamaño medio.

Caso práctico

1 Pequeña organización

Una empresa necesita mecanizar su trabajo administrativo mediante herramientas informáticas.

El ámbito geográfico de la empresa a la que nos referimos se reduce a la planta de un edificio.

Está organizada en dos departamentos: comercial y administración. El número total de puestos de trabajo que se han de mecanizar es de 15 personas: 10 en el departamento comercial y 5 en el de administración.

Los comerciales utilizan para su gestión software ofimático con correo electrónico, con objeto de realizar *mailings* y propuestas comerciales a sus clientes.

También utilizan una base de datos para la gestión de la cartera de clientes.

Los administrativos utilizan un paquete contable y software ofimático vinculado a la contabilidad. Tienen necesidad de imprimir formularios de gran tamaño y facturas.

Solución:

La carga de trabajo no es elevada, por tanto, con un único servidor departamental compartido por toda la empresa será suficiente.

Como los datos serán muy importantes, tendrá que elegirse un servidor tolerante a fallos o elegir un sistema de backup. Incorporaremos al servidor al menos dos discos, uno para el sistema operativo y otro para los datos de usuario.

Cuando el responsable del sistema haga backup, sólo tendrá que hacerlo con frecuencia del disco de datos. Las copias de seguridad del disco de sistema pueden espaciarse más y realizarse antes y después de hacer cambios en él.

La topología de red elegida puede ser una topología en anillo (Token Ring) entre todos los nodos de la red, puesto que las prestaciones solicitadas son moderadas.

Queda claro que hay que organizar al menos dos grupos de trabajo, uno por cada departamento.

Los comerciales no deben tener acceso a la información de los administrativos, porque utilizan información reservada (nóminas, facturación, etc.). Sin embargo, las impresoras del sistema sí pueden estar compartidas por ambos grupos.

Se requiere al menos una impresora matricial de carro grande para la elaboración de facturas, albaranes y formularios de gran tamaño. Además, se necesitará una impresora para imprimir las etiquetas de los *mailings* del departamento comercial.

Si los componentes de este departamento utilizan correo personalizado, necesitarán una impresora de mayor calidad y de mayores prestaciones. Es posible que haga falta más de una impresora de estas características. Los dos departamentos pueden acceder a todas las impresoras.

Sin embargo, los de administración encolarán trabajos a la impresora matricial con mayor prioridad que los comerciales, mientras que en la láser interesará que sea al revés.

Las aplicaciones de los comerciales residirán en las estaciones locales, de modo que puedan realizar gestiones comerciales independientemente de que el servidor esté o no en funcionamiento.

Sin embargo, la gestión administrativa residirá en el servidor, con objeto de que esté centralizada: una única contabilidad, un único procedimiento de copia de seguridad, etcétera.

Caso práctico

2 Organización de tamaño medio

Una empresa de artes gráficas necesita ampliar su sistema de red. Se parte de una configuración de Macintosh en red LocalTalk, sin ningún servidor. Dos impresoras LaserWriter están conectadas a puertos LocalTalk.

Por otra parte, la administración de la empresa utiliza tres PC compatibles aislados. Uno de estos PC incorpora un programa de conexión a una entidad bancaria para realizar transacciones financieras.

El crecimiento de la empresa exige incorporar las siguientes estaciones: una nueva planta con PowerMAC para el tratamiento de imágenes, una estación UNIX que controla un escáner de gran formato y una planta de PC para la composición de textos y el diseño de las páginas, dando cobertura a un nuevo grupo de clientes que entrega trabajos a imprimir en formatos de tipo PC.

Además, hay que instalar una filmadora conectada directamente a una red Ethernet.

Solución

Puesto que la filmadora debe conectarse a Ethernet, la red elegida para la instalación será Ethernet.

Colocaremos un *backbone* entre plantas basado en cableado estructurado por medio de conmutadores de alta velocidad (1 000 Mbps) que lleven líneas de par trenzado a cada una de las plantas. De cada planta se distribuirán a través de un concentrador nuevas líneas UTP para conexiones Ethernet en estrella a 100 Mbps.

A cada nodo le llegará una de estas líneas, con excepción de la estación UNIX, a la que llegará también un segmento de 1 000 Mbps puesto que su consumo de red será muy elevado, al tener que conducir un escáner de gran formato. También llegará un segmento de 1 000 Mbps a cada uno de los servidores.

Elegimos una configuración de tres servidores. El primer servidor será la propia estación UNIX, que necesitará grandes cantidades de disco para poder almacenar fotografías de alta resolución y en color. Este servidor no necesitará un sistema redundante: si se pierden los datos de un disco, bastará con leer de nuevo las fotos en el escáner; sin embargo, tendrá que disponer de un sistema de entrada/salida de alto rendimiento, porque tendrá que mover grandes cantidades de información. Podría convenir un sistema de discos con tecnología RAID de nivel 0. Además del TCP/IP incluido en UNIX, habrá que instalar un software añadido para la conectividad con redes AppleTalk, ya que los Macintosh y PowerMAC tendrán que leer y escribir información en este servidor.

Otro servidor debe proveer servicios al departamento de administración, que no tiene necesidades gráficas importantes.

Elegimos un pequeño servidor Novell que dará servicio a los PC de administración y que soportará las conexiones externas para las transferencias bancarias; además, incorporará la posibilidad de recibir pedidos automáticamente vía fax.

Los administrativos podrán utilizar el fax del servidor para automatizar sus envíos. El servidor debe tener tolerancia a fallos, pues la información que contendrá es crítica para la empresa. Como el servidor no requiere grandes prestaciones, bastará elegir un sistema de espejos entre dos discos.

El tercer servidor es el que utilizarán los talleres de tratamiento de textos e imágenes y proporcionará la conectividad entre los PC, Macintosh y PowerMAC. Uno de los PowerMAC actuará de encaminador entre el bus LocalTalk de los Macintosh y el resto de la red Ethernet, de modo que estén intercomunicados todos los nodos de cualquier segmento.

Este servidor tendrá mucho trabajo, por lo que interesará que sea un servidor con múltiples procesadores y tanta memoria RAM como sea posible. El sistema operativo de red elegido es Windows, que permite múltiples procesadores y conectividad a NetWare, a UNIX y a AppleTalk. La tarjeta de red deberá ser al menos de 1 000 Mbps para soportar todo el tráfico que a él se dirija.

Los discos de este servidor deben ser voluminosos y con sistema RAID de nivel 5, que permite tener seguridad y la posibilidad, en caso de fallo, de cambiar los discos en caliente, sin perturbar significativamente la producción de la empresa.No hay más remedio que seguir conectando las impresoras LaserWriter al segmento LocalTalk, puesto que no tienen otro tipo de puerto. Sin embargo, la filmadora se puede situar en cualquier punto de la Ethernet.

Probablemente hagan falta dos impresoras de alta producción compartidas en cada planta. Pueden estar conectadas a puertos de los servidores o, mejor aún, conectadas directamente a la red a través de un servidor especial que a veces incorporan las propias impresoras. Interesa que las impresoras sean PostScript, ya que es la misma tecnología utilizada por la filmadora y un lenguaje de descripción de páginas propiedad de Adobe apropiado para los sistemas de Apple. El intercambio de datos entre el servidor y AppleTalk se hará a través de AppleShare y LaserShare.

La red de Apple se configurará como dos zonas AppleTalk, una zona para los Macintosh (de moderadas prestaciones) y otra para los PowerMAC más la filmadora y el servidor.

Los usuarios de la red se configurarán como tres grupos: el primer grupo está constituido por los administrativos, que no tienen derecho de acceso más que a su servidor. El segundo grupo está constituido por la planta de PC y tiene derecho de acceso sobre todos los servidores con excepción del servidor NetWare. El tercer grupo es similar al segundo pero incluye a los usuarios de Macintosh y PowerMAC.

Conceptos básicos

- **Administrador de la red.** Es la persona encargada de las tareas de administración, gestión y seguridad en los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global. Este conjunto abarca tanto a servidores como a las estaciones clientes, el hardware y el software de la red, los servicios de red, las cuentas de usuario, las relaciones de la red con el exterior, etcétera.

- **Elementos del sistema de acceso a la red.** Básicamente son los siguientes: cuentas de usuario, contraseñas, grupos de cuentas, dominios y Directorio Activo o servicios de directorio, permisos y derechos, perfiles de usuario, sistemas y métodos de autenticación, etcétera.

- **Virtualización del almacenamiento.** Es un sistema que permite generar y administrar volúmenes virtuales (lógicamente simulados) a partir de volúmenes físicos en disco. Para el administrador del sistema, los discos virtuales pueden reasignarse sin esfuerzo y sin realizar modificaciones físicas en el hardware ni interrumpir las aplicaciones en ejecución. Adicionalmente, un sistema de virtualización significa una sencillez en la administración del almacenamiento.

- **Estándar Fibre Channel.** Este estándar es capaz de transportar los protocolos SCSI, IP, IPI *(Intelligent Peripheral Interface)*, HIPPI *(High Performance Parallel Interface),* los protocolos IEEE 802, e incluso, ATM. Se puede aplicar, por tanto, a redes locales, redes de campus, conjuntos asociados de ordenadores (clusters), etc. La distancia máxima permitida por esta tecnología es de 10 Km.

- **Subsistemas para las redes de almacenamiento de datos.** El primer sistema es el tradicional de almacenamiento de conexión directa (*Direct Attached Storage,* DAS), en el que cada estación de red tiene sus discos y los sirve a la red a través de su interfaz de red. Un segundo modo es el de almacenamiento centralizado *(Centralized storage),* en el que varios servidores o estaciones pueden compartir discos físicamente ligados entre sí.

  Los dos modos restantes son auténticos subsistemas. Se trata del almacenamiento de conexión a red (*Network Attached Storage,* NAS), en el que los discos están conectados a la red y las estaciones o servidores utilizan la red para acceder a ellos. Mucho más avanzado se encuentra el subsistema de redes de área de almacenamiento (*Storage Area Network,* SAN), que es una arquitectura de almacenamiento en red de alta velocidad y gran ancho de banda creada para aliviar los problemas surgidos por el crecimiento del número de los servidores y los datos que contienen en las redes modernas. SAN sigue una arquitectura en la que se diferencian y separan dos redes: la red de área local tradicional y la red de acceso a datos.

- **Protocolo IPP** *(Internet Printing Protocol)*. El protocolo de impresión internet es el modo de utilizar tecnología web para transmitir ficheros para imprimir a una impresora compatible con esta tecnología. IPP utiliza HTTP para realizar estas transmisiones, lo que le hace muy interesante ya que puede atravesar los cortafuegos con los que las organizaciones se protegen sin necesidad de abrir nuevos puertos de comunicación que aumenten la superficie de exposición a riesgos innecesarios.

- **Sistemas tolerantes a errores.** Es aquél que está capacitado para seguir operando aunque se presenten fallos en alguno de sus componentes. La tolerancia a fallos está diseñada para combatir fallos en periféricos, en el software de sistema operativo, en la alimentación eléctrica de los equipos, etcétera.

- **Funciones básicas del cifrado.** Son tres funciones: confidencialidad por la que los datos sólo son legibles por quienes son autorizados, integridad para asegurar que los datos son genuinos y autenticación para garantizar la identidad de los interlocutores.

- **Certificado digital.** Es una credencial que proporciona una Autoridad de Certificación que confirma la identidad del poseedor del certificado, es decir, garantiza que es quien dice ser. Se trata de un documento electrónico emitido por una entidad de certificación autorizada para una persona física o jurídica con el fin de almacenar la información y las claves necesarias para prevenir la suplantación de su identidad.

- **Infraestructura de clave pública.** Una PKI (*Public Key Infrastructure*, infraestructura de clave pública) es un conjunto de elementos de infraestructura necesarios para la gestión de forma segura de todos los componentes de una o varias Autoridades de Certificación. Por tanto, una PKI incluye los elementos de red, servidores, aplicaciones, etcétera.

- **Información que documenta la red.** Mapas de red, de nodos y de protocolos; mapas de grupos, usuarios, recursos y servicios; calendario de averías; informe de costes y planes de contingencia.

Actividades propuestas

Para ampliar

1. Sistema operativo de red NetWare de Novell: instalación, configuración y comandos.
2. Sistemas operativos de red de Microsoft: Windows Server 2003, Windows XP Home y Professional, Windows 2000 cliente y servidor, Windows Me, etcétera.
3. El sistema operativo de red de Apple: MacOS X (versión cliente y servidor).
4. Gestión de redes en UNIX.
5. Configuración de redes en Linux.
6. Estudio detallado de los protocolos SNMP, RMON y DMI.
7. Sistemas de directorio NDS de Novell y Directorio Activo de Microsoft.
8. Los dominios y Directorios Activos en Windows 2000 Server o superior.
9. Los sistemas de derechos de acceso entre distintos NOS: equivalencias entre ellos.
10. Sistemas comerciales de gestión de red.
11. Certificación digital.
12. Sistemas avanzados de autenticación.

Para buscar

1. www.computerprivacy.org
   Iniciativa *Americans for Computer Privacy*.
2. www.rsasecurity.com
   Sede web oficial de RSA.
3. www.pgpi.com
   Sede web internacional de PGP.
4. officeupdate.microsoft.com/office/redirect/fromOffice9/cert.htm
   Listado de algunas entidades emisoras de certificados.
5. www.cert.fnmt.es
   Sede web de CERES, Autoridad pública de CERtificación ESpañola, dependiente de la Fábrica Nacional de Moneda y Timbre.
6. www.ace.es
   Sede web de la Agencia de Certificación Española formada por Telefónica, SERMEPA, CECA y Sistema 4B.
7. www.sans.org
   Instituto SANS, notas sobre políticas de seguridad.
8. www.cerias.purdue.edu/coast
   Herramientas de software, archivos de información y proyectos de investigación sobre seguridad en la red.
9. www.kriptopolis.com
   Información sobre seguridad.
10. www.pgpi.com/download
    Sede de descarga de PGP, versión internacional.

Para realizar

1. No es fácil disponer en un laboratorio de una red SAN por el elevado coste que tienen, pero en las instalaciones empresariales de cierta entidad son muy utilizadas; por ello, es conveniente que profundices más en esta tecnología. Busca información para leer sobre ello en Internet. Puedes comenzar la búsqueda por la página: www.smdata.com/fcsan.htm
2. En la dirección web www.simple-times.org tienes mucha información sobre gestión de redes SNMP. En concreto es la sede web de una publicación periódica sobre este protocolo. Puedes descargar información desde allí en múltiples formatos para posteriormente hacer una lectura reposada.
3. Puedes complementar la información de la actividad anterior con tutoriales sobre gestión de redes que encontrarás en http://wwwsnmp.cs.utwente.nl/tutorials/
4. Como ya llevas unos cuantos meses de estudio de redes, te habrás dado cuenta de la necesidad de seguridad que toda red tiene. Comienza a elaborar un guión de sugerencias para mejorar posteriormente la seguridad de la red que utilizas.

Actividades complementarias

1. Fíjate en las fichas de creación de usuarios en Windows y en un sistema Linux para establecer analogías y diferencias entre las cuentas de usuarios en estos dos sistemas.

2. Ahora realiza el ejercicio anterior haciendo que el sistema Windows sea un controlador de dominio de Windows que pertenezca a un Directorio Activo.

   Observarás que el número de atributos que define una cuenta de usuario de Windows ha crecido significativamente.

3. Vamos ahora a establecer una comparativa entre los distintos tipos de permisos que se pueden gestionar en los archivos de los distintos sistemas operativos.

   Para ello, crea un fichero en Windows y otro en Linux. Asigna permisos de usuario al fichero de Windows y al de Linux. Observa las analogías y diferencias entre los dos sistemas de permisos.

   Si ahora integras la estación Windows en un dominio de un Directorio Activo te darás cuenta que también puedes asignar permisos para los usuarios del dominio y no sólo para los usuarios locales.

4. Repite el ejercicio anterior en el caso de carpetas en vez de ficheros.

   Busca información en Internet sobre las tecnologías de almacenamiento NAS Y SAN. Establece analogías y diferencias.

   Elabora un documento técnico que resuma las características básicas de cada uno de estos sistemas de almacenamiento.

   Busca soluciones comerciales de sistemas NAS de almacenamiento y lee las especificaciones técnicas de estas soluciones comerciales.

5. Busca información en Internet sobre la tecnología iSCSI que se suele utilizar en algunos de los sistemas de almacenamiento SAN. Elabora un documento técnico descriptivo de la tecnología.

   Elabora un informe con las características técnicas y precios de distintos modelos de SAI. Tendrás que estructurar esta tabla de datos por rangos de consumo: no se pueden comparar SAI para uso doméstico con SAI para uso en un Centro de Proceso de Datos.

   Fíjate especialmente en los sistemas de gestión remota del SAI.

6. Confecciona un documento técnico que describa las características básicas de los distintos modelos de RAID. Busca información en Internet sobre qué tecnologías RAID están soportadas por los distintos sistemas operativos de red.

   También existen tarjetas controladoras de discos SCSI capaces de gobernar sistemas RAID de discos. Busca algunas de ellas en Internet y fíjate en sus características técnicas y sus precios.

7. Estudia detenidamente la documentación de VNC y de Remote Administrator y elabora una tabla de decisión de cuándo utilizarías VNC y cuándo Remote Administrator.

   Instala estas aplicaciones en dos ordenadores para probar conexiones recíprocas. Prueba a realizar estas conexiones variando los diferentes parámetros de conexión, tanto gráficos (número de colores de la pantalla) como de comunicaciones (número de puerto de conexión).

8. Consigue en Internet información sobre las tecnologías WOL y ACPI para estudiar sus características básicas.

   Ahora busca placas madre de ordenadores personales que sean compatibles con estas tecnologías y compáralas.

9. Busca documentación técnica sobre PGP. Descarga el software PGP e instálalo en un equipo conectado a la red. Sigue la documentación técnica y prueba a enviar y recibir correos electrónicos cifrados con PGP.