

4

Unidad

Despliegue y mantenimiento de los servicios de red



En esta unidad aprenderemos a:

- Configurar los servicios básicos de discos e impresoras compartidas en la red.
- Gestionar el acceso a los servicios de infraestructura de redes IP.
- Utilizar la tecnología IP para montar servicios de colaboración entre usuarios.

Y estudiaremos:

- El funcionamiento de los servidores de asignación de direcciones y de resolución de nombres de la red.
- Las posibilidades de los sistemas operativos de red para compartir recursos de discos e impresoras.
- Los protocolos de alto nivel utilizados por los servicios de red.



CEO

S M R _ R L _ A A b a d _ 0 4 _
DespliegueAplicaciones.docx
Documento que contiene información sobre:

1. Aplicaciones de escritorio y distribuidas.
2. Despliegue de aplicaciones.

1. Recursos compartidos en la red

Desde el punto de vista de los usuarios, una red de área local se caracteriza por los servicios que presta. Algunos de estos servicios son transparentes para el usuario, aun siendo imprescindibles para la buena organización de la red. Un ejemplo de ello son los servicios de resolución de nombres de dominio de Internet.

Otros servicios están orientados al usuario hasta el punto de que las aplicaciones que utiliza no son más que clientes de estos servicios: es el caso del correo electrónico.

Un recurso de red es un elemento lógico capaz de realizar una acción a petición de alguien que lo solicita. El recurso recibirá el calificativo de compartido si la petición puede ser realizada a través de una red. De este modo, un recurso se convierte en el beneficio que provee un servicio.

Todo recurso se localiza físicamente en un nodo de la red concreto. Cuando compartimos un recurso, lo que se hace es virtualizar el recurso, es decir, dotarlo de las características técnicas necesarias para que parezca que es local al usuario que lo utiliza con independencia del sistema que realmente lo aloja. Así, cualquier nodo de la red podrá beneficiarse del servicio de modo transparente.

1.1. Discos, carpetas y ficheros

El recurso compartido más solicitado en la mayoría de las redes de área local son los discos y, más concretamente, las carpetas y ficheros que se encuentran en ellos. La elección correcta de estos discos influirá positivamente en la velocidad y en la seguridad del sistema.

A. Gestión de los discos

En el caso de servidores, interesan interfaces rápidas, por ejemplo, discos SCSI, especialmente las últimas versiones de esta tecnología (Ultra/Wide SCSI). En las estaciones de trabajo basta con interfaces IDE, Serial ATA o similares.

Los sistemas de almacenamiento modernos hacen 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.

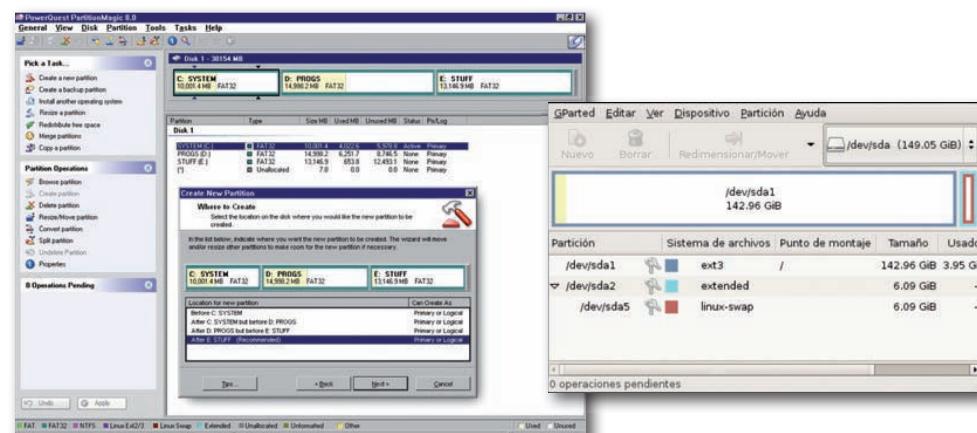


Fig. 4.1. Consola de una conocida marca de programa gestor de particiones de volúmenes para Windows (a la izquierda). Su equivalente de software libre, GParted, sobre Linux (a la derecha).



CEO

Especial importancia cobra la tecnología **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 son redes que conectan virtualmente grandes cantidades de almacenamiento en disco con los servidores de la red a través de una red de características especiales para facilitar esta función y que está separada de la red de área local que provee del resto de servicios de red.



CEO

S M R _ R L _ A A b a d _ 0 4 _
EstandaresDiscosRed.docx
Documento que contiene información sobre:

1. Estándar Fibre Channel.
2. Estándar iSCSI.



Caso práctico 1

Servir una carpeta en Windows y en Linux

Supongamos que una compañía despliega una división de comerciales que se dedican a la venta de medicamentos. El comercial sanitario toma cada día su PC y concierta un conjunto de visitas con diversos profesionales sanitarios para explicarles y documentarles el catálogo de productos que comercializan. Estos comerciales viajan por una extensa geografía y fotografían el exterior del centro sanitario que visitan para elaborar en las oficinas centrales un catálogo de centros sanitarios visitados con los contactos médicos realizados.

Una vez que los comerciales han regresado a las oficinas centrales, vuelcan esas fotografías en una carpeta de red que los profesionales de las relaciones públicas ponen a

su disposición para recogerlas y elaborar con ellas el catálogo.

Vamos a estudiar cómo compartir recursos de ficheros en un sistema Windows y en otro sistema Linux, algo que el administrador de la red tendría que realizar sobre el servidor en donde se vaya a compartir la carpeta.

Primero hay que preparar el disco que contenga la carpeta que vamos a compartir. Posiblemente habrá que formatear el disco para que quede limpio. El procedimiento de formateo creará el directorio raíz del disco. Compartir el disco significa compartir la carpeta raíz. Sin embargo, no es necesario compartir la carpeta raíz, podemos compartir cualquier otra carpeta.

Crearemos la carpeta que vamos a compartir y visualizaremos la ficha de compartir con el botón derecho del ratón una vez seleccionada la carpeta que se va a compartir.

Desde el menú contextual, tanto en Windows como en Linux, especificaremos el nombre del recurso compartido, es decir, cuál será el nombre para los usuarios de la red de esta carpeta. En el ejemplo de la figura, hemos creado una carpeta denominada «Imágenes corporativas» en el volumen físico Z y la vamos a compartir en la red con el nombre «Figuras».

En el caso de Linux, hemos llamado a este recurso compartido «OtrasFotos».

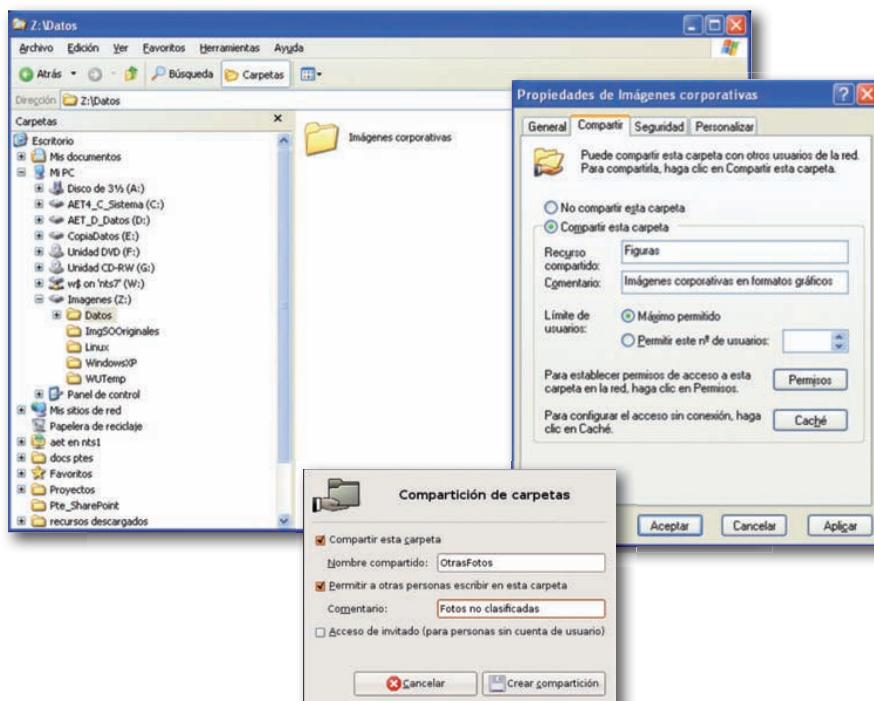


Fig. 4.2. Uso compartido de carpetas en Windows (arriba) y en Linux (abajo).

También tenemos que asignar permisos al recurso. Los permisos posibles son leer, cambiar y control total. Estos permisos indican qué es lo que los usuarios pueden realizar como máximo con los ficheros y carpetas que encontrarán dentro del recurso (Fig. 4.3, a la izquierda). Sin embargo, una vez alcanzado el recurso, el acceso a un fichero determinado lo marcarán los permisos del fichero o la carpeta concreta. Hay que conocer detalladamente cómo son los permisos del sistema de ficheros del sistema operativo que estemos utilizando para poder tener garantías de una cierta seguridad.

En Linux, el icono cambia según la distribución elegida, e incluso en algunas de ellas se puede elegir el icono. Aquí termina la operación en el servidor.

El cliente tiene que efectuar una conexión al recurso compartido para poder beneficiarse del servicio. Para efectuar una conexión remota a un servicio de disco tendremos que ejecutar el asistente de conexión a red desde el botón derecho del icono de red del sistema.

Continúa...



Caso práctico 1

...Continuación

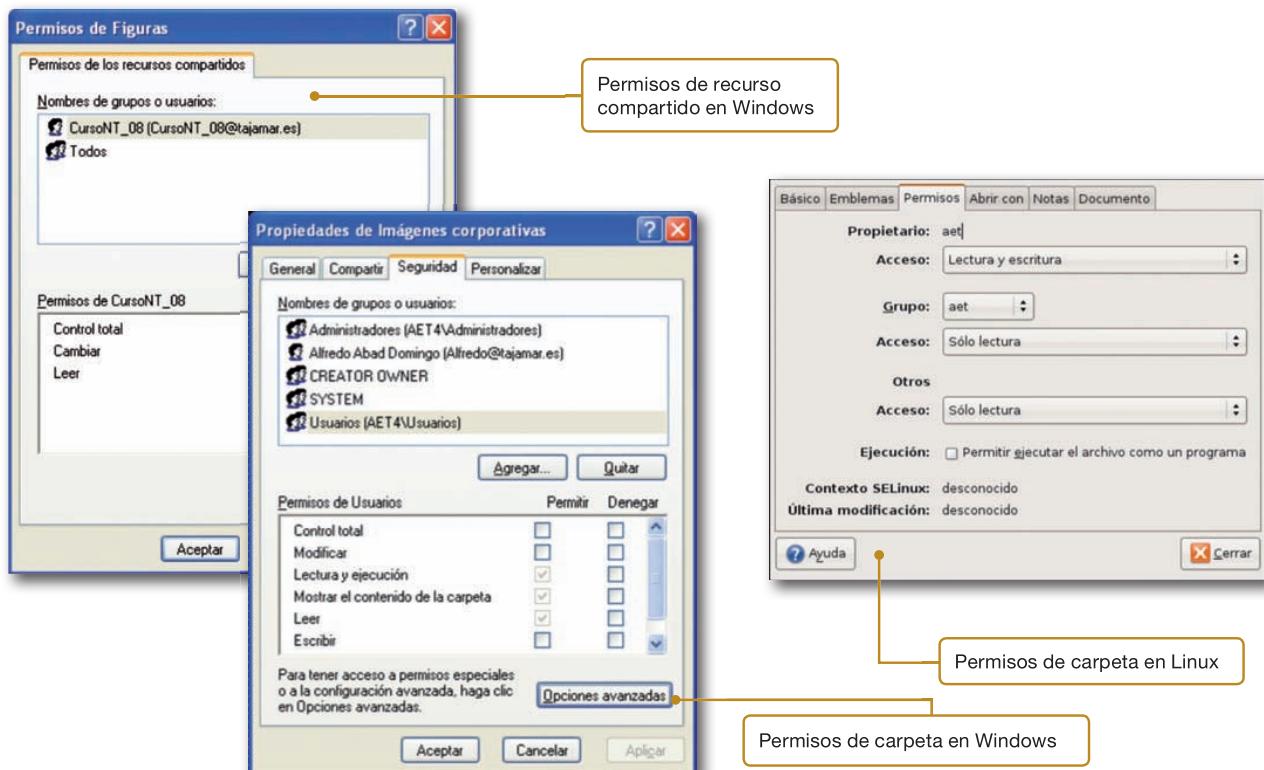


Fig. 4.3. Ficha de permisos de recursos y carpetas en Windows (a la izquierda) y de carpeta en Linux (a la derecha).

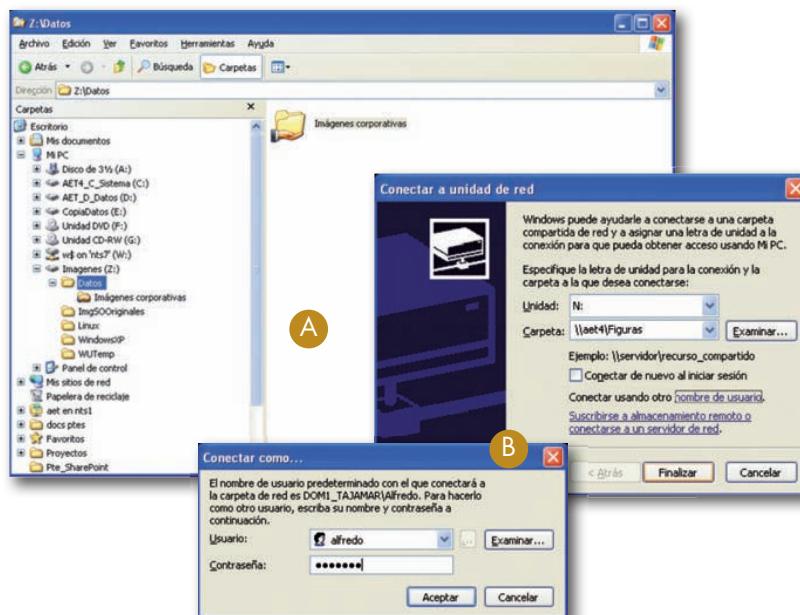


Fig. 4.4. A) Aspecto para el sistema operativo servidor de una carpeta compartida. B) Fichas de conexión a la carpeta compartida desde un cliente de red.

Indicaremos cómo queremos que se llame la unidad compartida en nuestro sistema («N:» en la Fig. 4.4-B) y la identificación del servicio, que se compone del nombre del servidor y del recurso compartido (en nuestro caso, \\AET4\Figuras). Si el recurso requiere identificación, podemos indicarle el nombre de usuario y contraseña que utilizaremos para acceder al servidor (tiene que ser una cuenta que resida en el servidor del recurso o a la que el servidor tenga acceso).

Después de esto se abrirá remotamente una carpeta en el cliente con el contenido del recurso como si la carpeta fuera local, a la que accederemos por el nuevo nombre de la unidad de red, que en nuestro caso es N.

Si tanto el servidor como el cliente usan los mismos protocolos para compartir recursos, no importará que tengan instalado Windows o Linux.

Continúa...



Caso práctico 1

...Continuación

Para completar el proceso de compartición, en la Fig. 4.5 se puede ver cómo se comparten carpetas en Windows 7. Hay dos modos de hacerlo: uno básico al que se accede desde el

botón Compartir que aparece en la ventana de propiedades haciendo clic con el botón derecho del ratón y una más avanzada, accesible desde el botón Uso compartido avanzado.

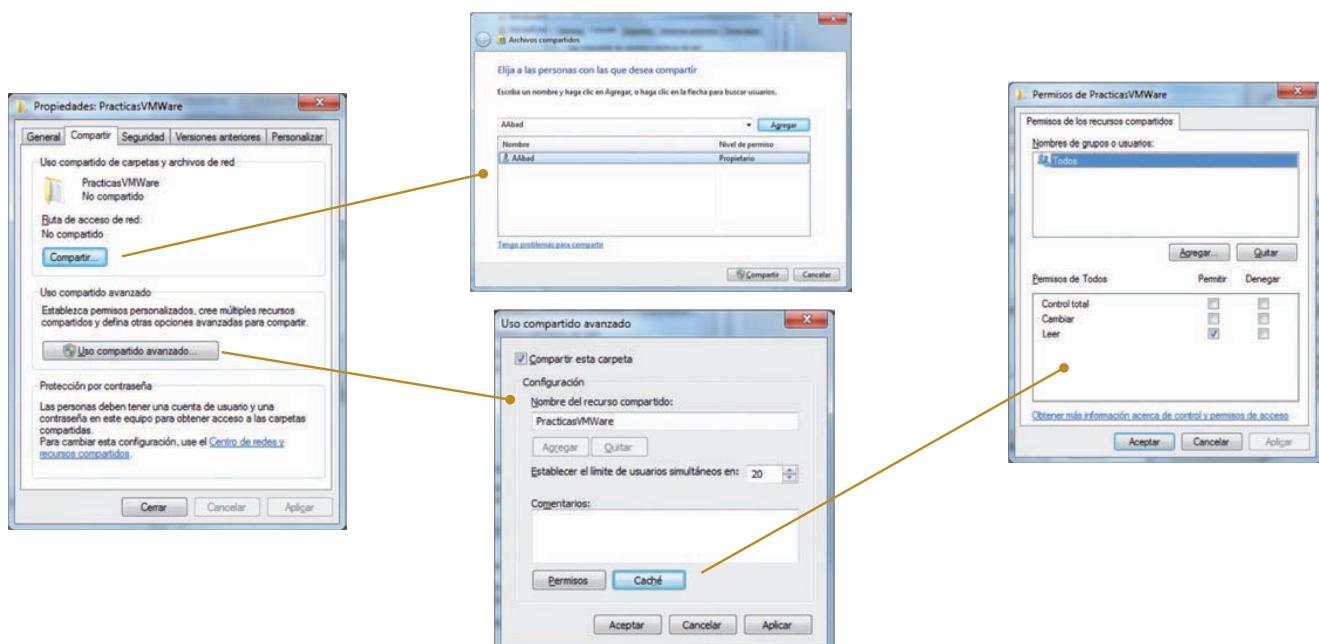


Fig. 4.5. Vista de la configuración del proceso de compartir carpetas en Windows 7.

1.2. Recursos de impresión de documentos

No todos los usuarios de una red tienen a su disposición dispositivos de impresión en sus ordenadores locales. Las redes facilitan que estos dispositivos se puedan compartir. Las redes de área local permiten a los clientes la conexión a las impresoras disponibles en toda la red y en 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.

Existen servidores de impresión expresamente dedicados a este tipo de tareas que gestionan todas las tareas de impresión con arreglo a unos parámetros concretos: velocidad de impresión, calidad de impresión, privilegios, prioridades, costes, etc.

Un buen diseño del sistema de impresión redundante 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.

IPP o *Internet Printing Protocol* (Protocolo de Impresión Internet) es el modo de utilizar tecnología web para transmitir ficheros de impresión a una impresora compatible con esta tecnología. IPP utiliza el protocolo típico de páginas web (*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. Además, es una tecnología transparente al sistema operativo: dará igual que sea Windows o Linux.



CEO

S M R _ R L _ A b a d _ 0 4 _
ImpresorasRedFax.docx

Documento que contiene información sobre:

1. Impresoras IPP.
2. Impresoras conectables a la red.
3. Servicios de fax.



Claves y consejos

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, etc.

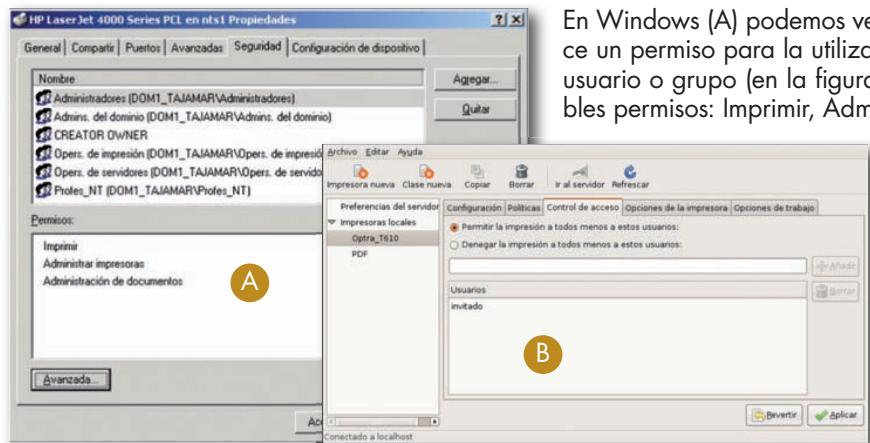


Fig. 4.6. Asignación de permisos para un recurso de impresión en Windows (A) y en Linux (B).

los usuarios y grupos sobre los que se establecen las autorizaciones de la impresora. Una vez seleccionado un grupo (por ejemplo el grupo de Administradores), caben tres posibilidades: Administrar impresoras y Administrar documentos.

En Linux (B) también se puede elegir el permiso o denegación de permisos a un conjunto formado por grupos y usuarios. Sin embargo, como se puede ver, el sistema de permisos se reduce a imprimir o no poder imprimir, que es más pobre que en Windows, en donde también podemos establecer que se puedan administrar los trabajos y la misma impresora.

Caso práctico 2

Creación de una impresora compartida

Seguimos con el ejemplo anterior de los comerciales sanitarios. En sus viajes han generado gastos que deben ser comunicados al departamento de contabilidad para que se proceda a su gestión. Cada comercial ha ido tomando apuntes de gastos en una hoja de cálculo. Cuando vuelven a las oficinas centrales, cada comercial se conecta a una impresora de red que tiene el departamento de contabilidad y envía a esa impresora su hoja de gastos. El administrador de red tendrá que haber creado previamente un recurso compartido de impresión con permisos de imprimir para todos los comerciales.

Windows tiene un panel de control denominado Impresoras y faxes. Desde este panel se arrancan todos los asistentes de configuración de impresoras, tanto locales como de red.

Para crear un recurso de impresión hemos de crear una impresora local y luego compartirla en la red. La creación de la impresora exige ejecutar el asistente de Agregar una impresora y después seguir las instrucciones del asistente. Indicaremos el puerto local por el que el sistema se comunicará con la impresora, por ejemplo, por el puerto paralelo LPT1, aunque los sistemas modernos permiten también especificar puertos remotos.

Seguidamente especificaremos la marca y modelo de la impresora. Si el sistema operativo no contempla este modelo, tendremos que recurrir al software que el fabricante nos habrá proporcionado con la impresora.

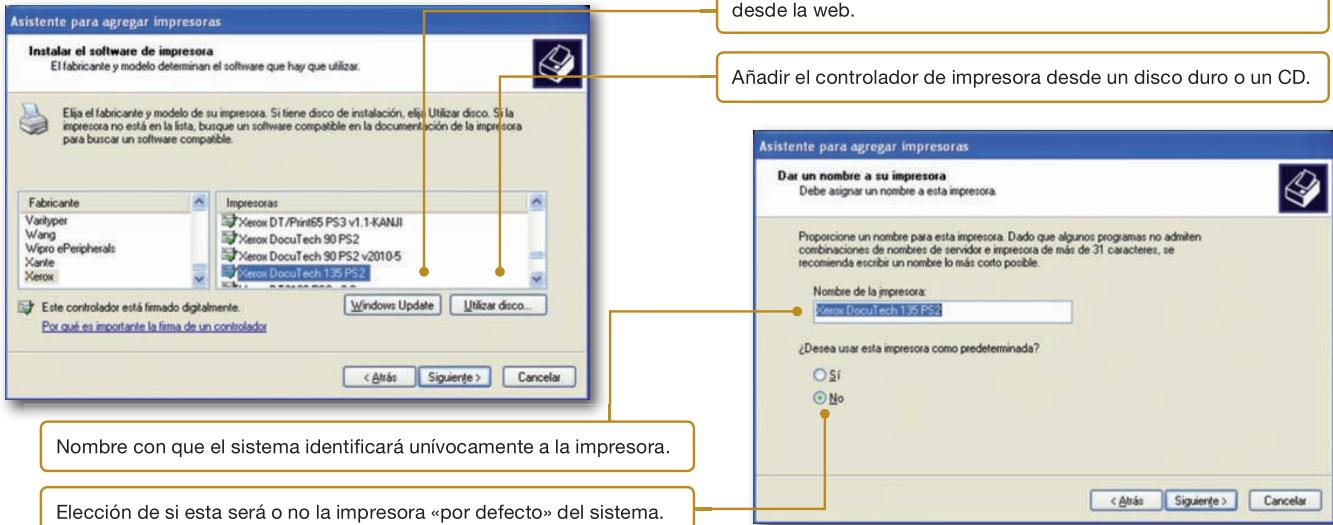


Fig. 4.7. Ventanas de selección del controlador de impresora (A) y asignación del nombre de la impresora (B).

Continúa...



Caso práctico 2

...Continuación

El asistente instalará el software necesario e invitará a probar la impresora. Una vez que tengamos la impresora recién instalada funcionando correctamente en local, habrá que compartirla para la red.

Desde las propiedades de la impresora podemos acceder a la ficha Compartir en donde especificaremos el nom-

bre con el que será conocida en la red. Si el servidor de la impresora está integrado en un dominio Windows, el asistente nos permitirá incluir la impresora en el Directorio Activo, de modo que posteriormente los clientes de la impresora la puedan buscar en el Directorio Activo en que se integran.

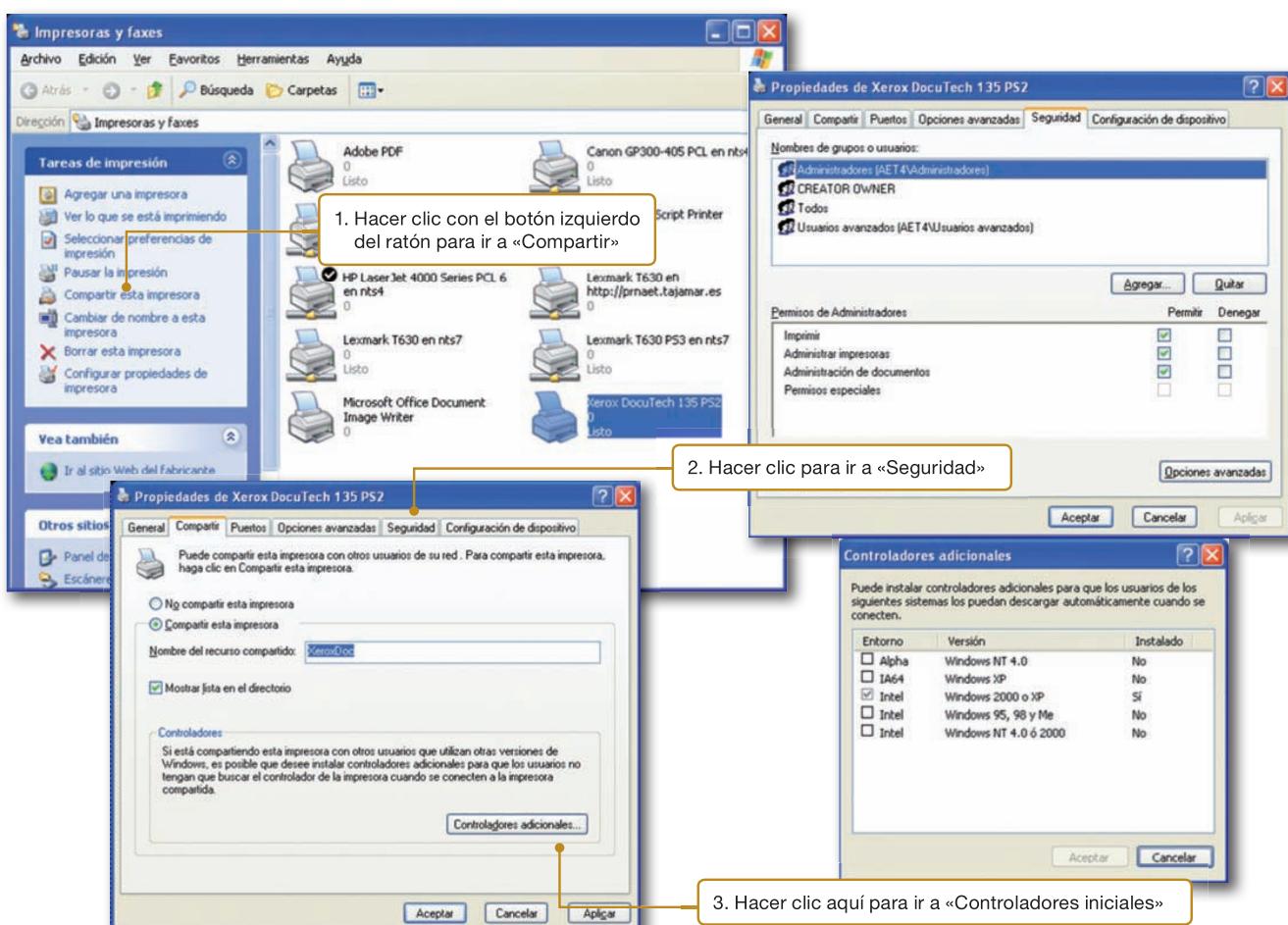


Fig. 4.8. Ventanas de creación de un recurso de impresión compartido, seguridad y controladores adicionales.

Como la impresora será utilizada por los clientes de la red, que pueden tener un sistema operativo distinto al del servidor, Windows nos permitirá especificar qué sistemas operativos clientes tendrán en la red e instalará una copia del controlador de impresoras para cada uno de estos sistemas cliente. Cuando un cliente se conecte a la impresora, si no tiene el controlador adecuado, el servidor Windows de la impresora se lo proporcionará automáticamente (ficha de controladores adicionales).

Después, podremos asignar los permisos a la impresora compartida desde la ficha de Seguridad: será algo semejante a la seguridad para los recursos compartidos de disco.

Podemos comprobar que, efectivamente, la impresora que acabamos de compartir ha sido registrada en el Directorio Activo y que, por tanto, cualquier cliente que participe de ese servicio de directorios podrá encontrar la impresora de red.

Continúa...



Caso práctico 2

...Continuación

Hasta aquí lo que el administrador de red tiene que hacer en el servidor que brinde la impresora a la red.

Ahora nos vamos a enfrentar a la tarea de cada cliente, en nuestro caso, los comerciales que deberán abrir remotamente la impresora de red para ser utilizada desde sus portátiles.

Si nos presentamos en un cliente de la red que participe del Directorio Activo y tratamos de agregar una impresora de red, el asistente nos facilitará varias posibilidades: impresora local, impresora remota o una impresora residente en el Directorio Activo (Fig. 4.9-A).

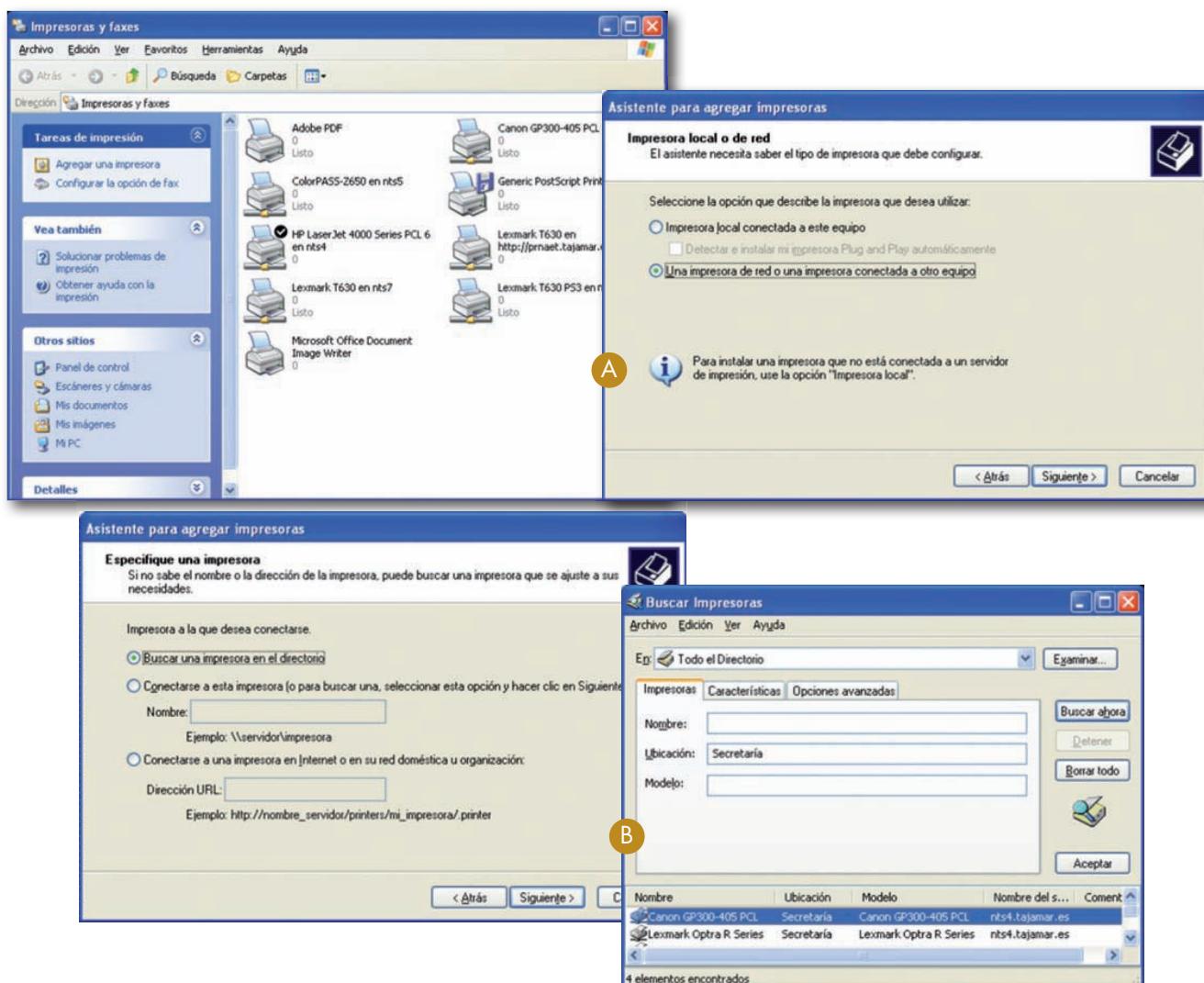


Fig. 4.9. A) Conexión a una impresora de red. B) Búsqueda de una impresora en el Directorio Activo.

Especificamos las opciones de búsqueda, que en la Fig. 4.9-B han sido todas las impresoras ubicadas en Secretaría, y nos presentará las impresoras solicitadas. Seleccionando la que queramos, podremos conectarnos a ella con la opción de Conectar desde el botón derecho del ratón.

También podemos realizar la conexión a la impresora directamente si conocemos el nombre del recurso de impresión, justo la denominación con la que el administrador de la red compartió la impresora.

Continúa...



Caso práctico 2

...Continuación

Estos nombres toman el aspecto de un recurso NetBIOS, es decir, \\NOMBRE-DE-SERVIDOR\RECURSO-COMPARTIDO. El asistente nos puede presentar el explorador de la red para poder seleccionar alguno de los recursos de impresión compartidos en toda la red (Fig. 4.10). En el caso de nuestra figura el recurso compartido sería

\\nts4\CanonGP3, que soporta una impresora modelo Canon GP300-405 con lenguaje gráfico PCL.

Si el recurso existe en la red y el comercial tiene recursos de acceso a él, entonces podrá utilizar la impresora de red exactamente igual que si fuera una impresora local conectada a alguno de los puertos de su portátil.

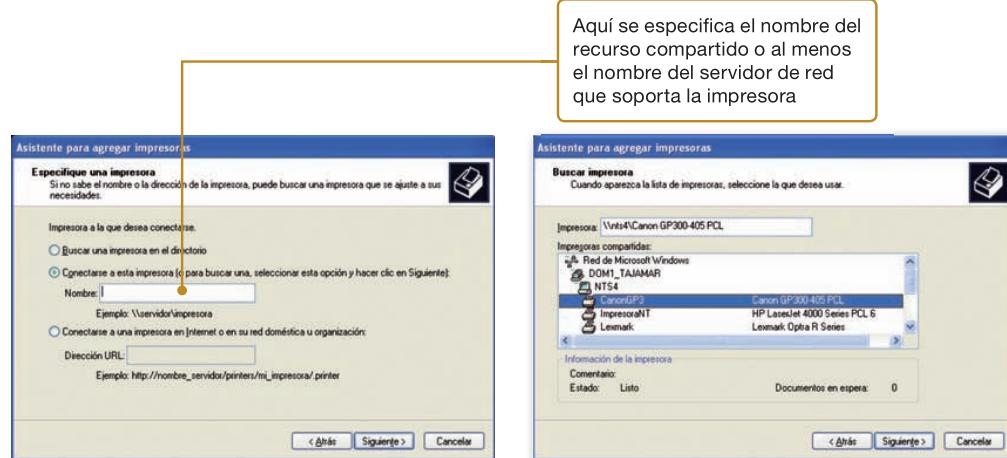


Fig. 4.10. Búsqueda de una impresora en toda la red sin utilizar el Directorio Activo.

En el caso de Linux es posible acceder a la gestión de las impresoras desde el panel de control de impresoras en donde se podrán configurar tanto impresoras locales como remotas a través de un servidor de red remoto. Si se crea una impresora local, esta se podrá compartir a través de

la red. Si se crea una impresora remota, entonces el cliente intentará una conexión con un dispositivo situado al otro lado de la red, compartido a través de un software servidor (servidor de impresoras).

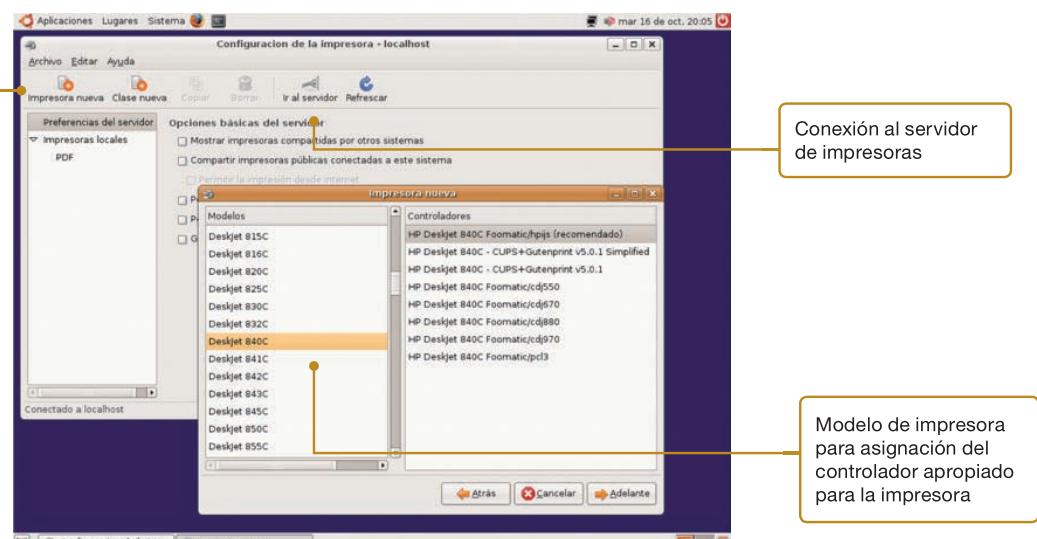


Fig. 4.11. Configuración de impresoras locales o remotas en Linux.

**Ampliación**

Los servidores DNS actuales no solo registran nodos de la red sino que también pueden dar de alta en su base de datos otros servicios, de modo que un nodo de la red puede preguntarle dónde se encuentran los servicios que necesita dentro de su red.

2. Servicios de infraestructura TCP/IP

No todos los servicios de la red tienen una incidencia tan clara en el trabajo ordinario de los usuarios como los vistos anteriormente. La mayor parte de los servicios de red son utilizados por los usuarios y por las aplicaciones que ejecutan con total transparencia: este es el caso de los servicios de infraestructura TCP/IP.

2.1. Servidores DNS

DNS (*Domain Name System*, sistema de nombres de dominio) es un sistema de articulación de nombres para nodos TCP/IP que intenta organizar de modo jerárquico el nombre de todos los nodos conectados a una internet. Se trata de memorizar nombres, que es más sencillo que números (direcciones IP).

Cada nombre DNS consta de dos partes. La primera parte identifica al nodo dentro de una subred. La segunda parte identifica a la subred y se llama dominio. La proliferación de nodos en Internet ha creado la necesidad de fraccionar los dominios en subdominios de uno o varios niveles.

Cada uno de los niveles (dominio, subdominios y nodos) va separado del siguiente nivel en la escritura del nombre por un punto. Por ejemplo, si tomamos el nombre DNS **venus.solar.vialactea.univ**, entonces queda identificado el nodo **venus**, integrado dentro de un sub-subdominio llamado **solar**, en el subdominio **vialactea** del dominio **univ**.

En una red TCP/IP compleja deben definirse en cada nodo las direcciones IP de los servidores DNS que resuelven los nombres de red cuando ese nodo tiene necesidad de ello. Estrictamente solo es necesario un servidor DNS; sin embargo, por motivos de seguridad suelen asignarse dos o más. Al primer DNS se le llama DNS primario.

Se han desarrollado versiones de DNS denominadas DDNS (*Dynamic DNS*) o DNS dinámico, que permite que los nodos registren automáticamente los nombres de sus equipos, enlazándolos con sus direcciones IP en un servidor DNS. Así, en un DDNS de Microsoft no solo se registrarán nodos IP, sino todo aquello que deba poderse localizar en una red: servicios de disco, impresoras, directorios activos, etc. En la Fig. 4.12 podemos ver un ejemplo de DDNS.

**Actividades**

1. Confirma la veracidad de las siguientes afirmaciones:
 - a) Los servicios de discos de red pueden compartir carpetas de red, pero no ficheros individuales.
 - b) Es recomendable que a los servicios de disco compartidos en la red se acceda anónimamente.
 - c) iSCSI es una tecnología para conexión de grandes volúmenes de discos a los servidores utilizando una red IP como medio de transporte.
 - d) En una red de área local no se puede imprimir con tecnología IPP.
 - e) El nombre de un recurso de impresora de red sigue el formato \\SERVIDOR\\IMPRESORA.
 - f) El nombre de un recurso de disco compartido en red sigue el formato: \\NOMBRE-SERVIDOR\\DIRECCION-IP.
2. Razona brevemente cómo puede ser que un servidor que comparte una impresora de red pueda gestionar los controladores de la impresora de red para clientes

de diversos sistemas operativos, por ejemplo, distintas versiones de Windows y Linux.

3. Elige un PC que pertenezca a una red local que hará las funciones de servidor y otro PC en la misma red que hará las funciones de cliente. Crea en él una carpeta en uno de sus discos. Asignale permisos de lectura y escritura para un usuario que crees con antelación y que denominaremos UsuarioCliente. Luego, realiza las siguientes actividades:
 - a) Comparte la carpeta recién creada a la red con el nombre de recurso «Compartido».
 - b) Comprueba que desde el PC cliente puedes abrir remotamente esta carpeta compartida del servidor.
 - c) Si no existe ya una impresora local, instala una impresora local en el PC servidor. Ahora, compártela en la red para que pueda ser utilizada por el UsuarioCliente.
 - d) Comprueba que puedes utilizar la impresora de red desde el PC cliente.

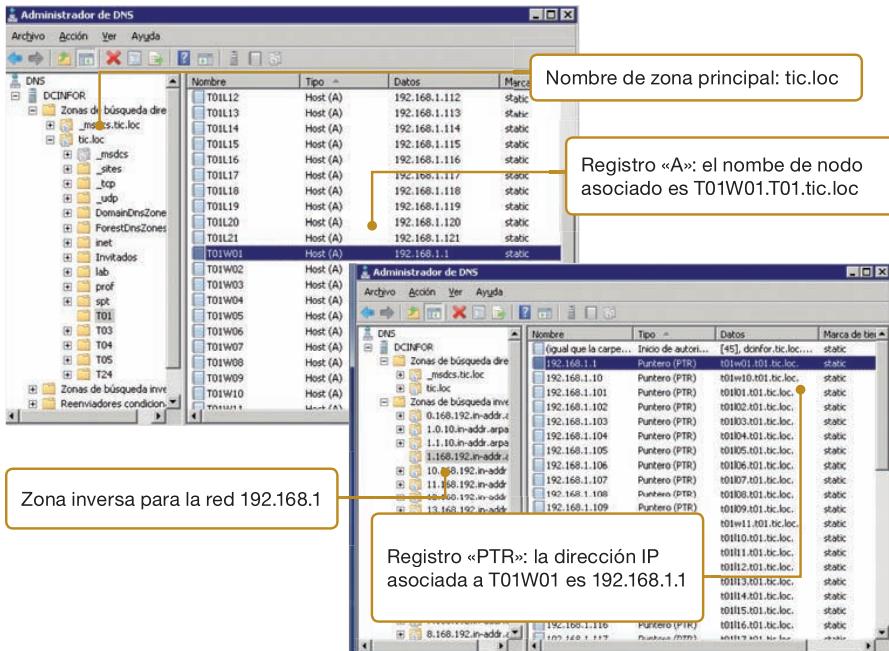


Fig. 4.12. Representación gráfica de un servidor DNS sobre un servidor Windows Server 2008 R2: zona directa (izquierda) y zona inversa (derecha).

Los servidores Windows incorporan software para la explotación de un servidor DNS sin necesidad de una licencia añadida. En el entorno Linux, el servidor DNS de software libre por antonomasia es bind9, que no tiene un entorno gráfico amigable pero que no por ello deja de ser muy potente y flexible. Su configuración reside en un conjunto de ficheros que describen las zonas DNS y los nombres de los hosts que se inscriben en ellas.

En la Fig. 4.13 hay un ejemplo de configuración de dos de los ficheros importantes de bind9 que describen zonas de búsqueda directa e inversa. Las zonas directas resuelven nombres DNS en direcciones IP, mientras que las zonas inversas traducen direcciones IP a nombres DNS.

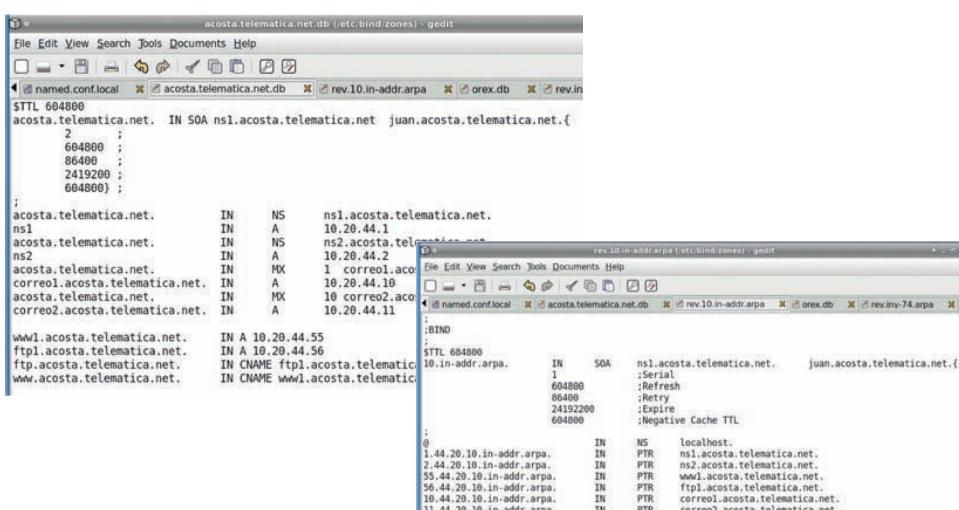


Fig. 4.13. Vista del fichero de configuración en bind9 de una zona DNS directa (izquierda) y otra inversa (derecha).

En cada servidor DNS se crean una o más zonas. Cada zona va asociada a un identificador que normalmente es un subdominio y un dominio. Dentro de cada zona se dan de alta registros de diversos tipos. El registro más común es el de tipo «A» que asocia nombres de nodos con direcciones IP. Las zonas inversas son las que se encargan de la relación inversa, es decir, a partir de una dirección IP consiguen un nombre de nodo.

Obsérvese que el nombre de las zonas inversas se expresa con los números de la red escritos en orden inverso.



Ampliación

Cuando un host necesita enviar datos a otro host, puede acceder a él por su dirección IP o bien a través de su nombre DNS, que será lo más común. Para utilizar el nombre DNS necesita hacer la conversión de este nombre en su dirección IP equivalente. De esto se encargan los servidores DNS. El host emisor envía un paquete de consulta a su DNS predefinido con el nombre DNS que intenta resolver, para que el servidor DNS lo resuelva o ejecute los mecanismos necesarios de consulta con otros servidores DNS, y le devuelva la dirección IP que necesitaba.

En sistemas UNIX, y por absorción tecnológica también en otros sistemas, existe un fichero de configuración llamado «/etc/hosts» que contiene una relación de asignaciones de nombres DNS con direcciones IP para los nodos de la red de área local. En Windows el fichero está situado en **C:\raíz_sistema\system32\drivers\etc**, mientras que en sistemas UNIX se sitúa en **/etc**.

Este es un modo de utilizar nombres DNS sin necesidad de tener acceso a un servidor DNS. Obviamente este fichero solo puede contener un número muy limitado de asignaciones, que además deben ser previamente conocidas para poder ser escritas por el administrador de red en el fichero de hosts.

**Truco**

En los sistemas Windows el nombre NetBIOS de un nodo coincide con el nombre del PC en que se instala el sistema operativo. En cambio, en los sistemas Linux en los que se configura el servicio NetBIOS es posible asignar el mismo nombre del PC u otro alternativo.

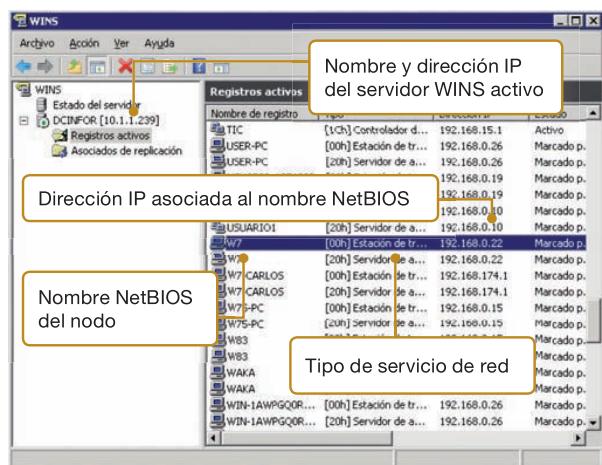


Fig. 4.14. Consola de administración de un servidor WINS sobre Windows Server 2008 R2.

2.2. Servidores de nombres WINS

DNS no es el único sistema de nombres para redes. Existen sistemas de nombres planos, no articulados, que identifican cada nodo de una red por un nombre único. Estos sistemas son especialmente eficaces en pequeñas redes o, en grandes redes, combinados con otros sistemas de nombres articulados.

El sistema de nombres planos más extendido actualmente viene determinado por los nombres propios de la interfaz NetBIOS. En ocasiones interesa enlazar los nombres NetBIOS de los equipos de la red con las direcciones IP de los mismos. WINS (Servicio de nombres Internet de Windows) es un servicio propio de redes de Microsoft que viene a resolver inteligentemente este problema evitando el tráfico de paquetes de difusión en gran medida.

El registro de un nodo en la base de datos de WINS es automático; basta con que el nodo registre su nombre NetBIOS para que se produzca el alta de la asociación entre nombre y dirección IP. La resolución de nombres NetBIOS tiene un archivo semejante al hosts de nombres DNS. Se trata del fichero LMHOSTS, que en Windows suele estar localizado en \raiz_sistema\SYSTEM32\DRIVERS\ETC\LMHOSTS.

En Windows, WINS también se integra con DNS estableciendo una correspondencia entre los dos sistemas de resolución de nombres. Si ambos servicios están activados, cuando un usuario pide un nombre de red, si el servicio al que se lo pidió no es capaz de resolverlo, este interrogará a su servicio homónimo, todo ello de modo transparente.

En la Fig. 4.14 podemos ver la consola de administración de un servidor WINS. En ella se ha solicitado al servidor que presente en pantalla las estaciones de trabajo y controladores de dominio de la red junto con las direcciones IP que llevan asociadas. Podemos distinguir que hay definidos nombres NetBIOS, por ejemplo, W7 que se relaciona con la dirección IP 192.168.0.22 y que soporta varios servicios de red: actúa como estación (entiéndase cliente) con el servicio 00h y como servidor con el servicio 20h.

**Truco**

También es posible la asignación estática de direcciones, es decir, se le puede decir al servidor DHCP que cuando la tarjeta de red con dirección MAC «x» le solicite una dirección IP, el servidor le asigne siempre una dirección IP reservada «y», lo que garantiza que esa tarjeta de red siempre tendrá la misma dirección IP.

**Ampliación**

El servidor DHCP va asignando las direcciones IP conforme los clientes lo solicitan, elegidas de un ámbito de asignación que previamente ha determinado el administrador de la red, de modo que dos clientes distintos no tengan la misma dirección IP, lo que produciría un caos en la red. En la mayoría de los servicios DHCP se pueden crear restricciones a estos ámbitos, de modo que haya direcciones IP reservadas y que, por tanto, no son asignables dinámicamente. DHCP tuvo originalmente un protocolo más primitivo que tenía unas funciones semejantes:

2.3. Servidores DHCP

La asignación de direcciones IP a todos los nodos de una red de área local puede ser muy laboriosa, sobre todo si el número de nodos es elevado o si tiene que estar conectada a otras redes de área local formando una red de área extendida.

El protocolo DHCP (*Dynamic Host Configuration Protocol* o protocolo de configuración dinámica de host), junto con los servicios DHCP, ayudan al administrador de la red para automatizar estas asignaciones haciéndolas dinámicas.

El servidor DHCP, a través del protocolo DHCP, asigna una dirección IP a cada nodo que lo solicita de modo que no pueda asignarse la misma dirección IP a dos nodos distintos de la red. Cuando el nodo IP cambia de red o se apaga, su dirección queda liberada y puede ser asignada por el servidor DHCP a otro nodo que lo solicite, una vez concluido un tiempo de reserva.

BOOTP (*Bootstrap Protocol*). El problema de BOOTP es que requería una configuración manual muy exigente que representaba una carga laboral importante para los administradores de red, además de una mayor probabilidad de cometer errores en la configuración. DHCP vino a resolver este problema. Puede conseguirse más información sobre BOOTP entre otros sitios en http://es.wikipedia.org/wiki/Bootstrap_Protocol y en http://www.tcpipguide.com/free/t_TCPIPBootstrapProtocolBOOTP.htm

Los modernos DHCP no solo asignan direcciones IP, sino que asignan muchos otros parámetros: encaminadores, servidores DNS, servidores WINS, servidores de correo, máscaras, servidores de tiempo, directorios, etc. Lo que es más común en las instalaciones de red en que se utiliza DHCP es que el servidor DHCP asigne dirección IP, máscara de red, puerta por defecto y servidores de resolución de nombres DNS o WINS.

En la Fig. 4.15 podemos observar cómo el servidor DHCP ha ido concediendo direcciones IP elegidas entre las disponibles en su ámbito (192.168.0.0) y, en concreto, ha asignado la dirección IP 192.168.0.22 a un nodo cuyo nombre NetBIOS es W7.invitados.tic.loc. El nombre DNS asignado para este nodo es W7.invitados.tic.loc.

También podemos apreciar dentro de la consola una carpeta denominada «Reservas» en la que se incluirán las asociaciones estáticas entre direcciones MAC y direcciones IP, si las hubiera.

En cada segmento de red solo puede haber un servidor DHCP, de lo contrario cuando un cliente DHCP haga una petición no tendrá modo de discriminar qué servidor le atenderá y ello puede dar problemas de direccionamiento en la red. Aun así pueden elegirse configuraciones especiales para tener dos servidores DHCP que sean redundantes sin que colisionen entre sí.

Los administradores de sistemas y de red deben ponerse de acuerdo para definir correctamente qué servidor DHCP atenderá a cada segmento de la red. Por otra parte, muchos dispositivos de red sencillos, como los puntos de acceso inalámbricos o los enruteadores domésticos, pueden habilitar servicios DHCP que pueden interferir con el servidor DHCP corporativo. En este caso hay que tener cuidado de deshabilitar el servicio DHCP en estos dispositivos de red si ya se posee otro corporativo.



Actividades

4. Comprueba si son ciertos o falsos los siguientes enunciados:
 - a) WINS es un servicio de los servidores Windows que asocia direcciones IP a nombres DNS.
 - b) DNS es un servicio exclusivo de servidores Linux.
 - c) La asociación entre nombres de equipos y direcciones IP se lleva a cabo en los servidores DNS.
 - d) Los servidores DHCP pueden conceder una dirección IP al equipo que lo solicita, pero nunca una máscara de red.
 - e) La dirección IP del servidor DHCP debe coincidir con la puerta por defecto del nodo que solicita la dirección.
5. Conéctate a la página <http://www.see-my-ip.com/tutoriales/protocolos/dhcp.php>. Encontrarás un tutorial sobre la conversación que mantiene un cliente DHCP con el servidor DHCP que le atiende hasta que le asigna sus parámetros de red. Después de leer atentamente este artículo, representa gráficamente la secuencia de pasos de esta conversación. Puedes ampliar los conocimientos en el artículo «DHCP» de Wikipedia.
6. Elige un PC que pertenezca a una red local que hará las funciones de servidor y otro PC en la misma red que hará las funciones de cliente. Asegúrate de que en el

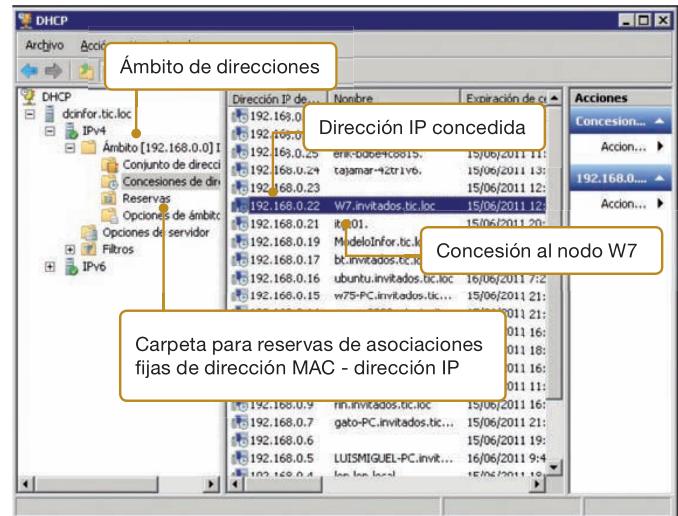


Fig. 4.15. Representación gráfica de un servidor DHCP sobre Windows Server 2008 R2.

servidor tienes instalado el software de servidor DNS (DNS Server en Windows o bind9 en Linux).

Luego, realiza las siguientes actividades:

- a) Crea una zona DNS con el nombre redes.locales.
- b) Crea un registro de tipo A para dar de alta el nombre del PC cliente con su dirección IP. Crea otro registro de tipo A para hacer lo mismo con el nombre y dirección IP del servidor.
- c) Abre una sesión en el PC cliente y asigna en sus parámetros de red que su servidor DNS es la dirección IP del servidor DNS. De este modo, su resovedor de nombres será el nuevo servidor DNS que acabamos de configurar.
- d) Haz un ping desde el PC cliente a la dirección DNS del PC servidor. ¿Se resuelven los nombres en direcciones IP?
- e) Asegúrate de que el servidor DNS de la red en el PC Servidor apunta a un DNS de la conexión de banda ancha hacia Internet. Comprueba que resuelve nombres externos, por ejemplo, haciendo un ping a www.google.com.
- f) Ahora, haz un ping desde el PC servidor al nombre DNS del PC cliente. ¿Consigues resolver el nombre DNS interno de PC cliente? ¿Por qué?



CEO

S M R _ R L _ A A b a d _ 0 4 _
ServiciosPublicacionInternet.docx
Documento que contiene información sobre:

1. Servidores web.
2. Servidores ftp.



Fig. 4.16. Apple iPhone con navegador de Internet.



Ampliación

Entre las principales ventajas que ofrece una Intranet se encuentran las siguientes:

- Mejora de las comunicaciones internas entre las personas de la organización debido a la simplificación del acceso a la documentación corporativa.
- Es posible el acceso a bases de datos de modo que los datos se plasman dinámicamente en los documentos que se visualizan. De este modo se garantiza que la información consultada es actual en cada momento.
- El acceso a la información es idéntico desde dentro y desde fuera de las instalaciones de las empresas ya que la tecnología utilizada para realizar la consulta es exactamente la misma.
- La tecnología Internet está muy probada, lo que hace que se disminuyan los riesgos de funcionamiento incorrecto o de obsolescencia tecnológica.

3. Intranet e Internet

Muchas corporaciones se han planteado la utilización de la tecnología Internet en la propia red de área local. La aplicación de los métodos y tecnologías de Internet en el ámbito local convierte a la LAN en una Intranet.

3.1. Globalización de la tecnología web

La utilización de tecnologías como HTML, XML, XHTML, lenguajes de programación como PHP, JavaScript, Python, ASP o plataformas de soporte de aplicaciones como Java o .Net Framework hace que las aplicaciones web sean muy complicadas desde el punto de vista de la instalación y de los protocolos de red que utilizan, pero a cambio facilitan la interoperabilidad y la flexibilidad. Muchas de estas tecnologías pueden interpretarse sobre distintas plataformas, tanto de software como de hardware.

Por ejemplo, la utilización de HTML y sus derivados hace que los documentos de la organización sean fácilmente portables entre los distintos equipos que componen la red de área local, facilitando que todos los documentos de la empresa estén codificados en un mismo formato.

Especial mención requiere todo el mundo de acceso a las redes sociales desde dispositivos móviles tan sencillos, pero a la vez tan sofisticados como los actuales teléfonos inteligentes (*smartphones*) o dispositivos de mano como los iPad, los PDA, etc.

La tecnología Intranet implica la utilización de las tecnologías propias de Internet en la propia red de área local, por ello para la construcción de una Intranet son necesarios los siguientes elementos:

- **Una red de área local.** La red de área local debe correr al menos el protocolo TCP/IP, básico en la tecnología Internet. Facilita el acceso a los servidores de la LAN la instalación de sistemas que resuelvan los nombres de la red, por ejemplo, un sistema DNS, WINS o cualquier otro que haga más cómodo el acceso a los diferentes recursos a todos los usuarios, sin necesidad de memorizar una lista de direcciones IP.
- **Clientes de red.** Todos los ordenadores que tengan acceso a la Intranet necesitan del protocolo TCP/IP, además de un navegador. En la medida en que el navegador sea más rico e incorpore más extensiones permitirá el acceso a un mayor número de documentos y tendrá mayor funcionalidad. Se admiten todos los dispositivos de red que permitan una conectividad a la red con capacidad de navegación.
- **Servidores de red.** Los servidores de Intranet son los proveedores de servicios telemáticos en la red de área local: web, FTP, etc. Cualquier puesto puede proveer un determinado servicio y, en virtud de esto, ser por ello considerado «el servidor» de ese servicio en particular con tal de que ese sistema admita el software necesario correspondiente al servicio.
- **Configuración del sistema.** Una vez instalado todo el hardware y software de la Intranet, es necesario un diseño de la ubicación de los documentos, su estructura jerárquica en forma de páginas que permitan la navegación y la definición de los permisos de acceso a cada una de ellas por parte de cada uno de los usuarios. Por último, habrá que instalar las aplicaciones de la Intranet y publicarlas en las páginas web que actuarán como frontales de los distintos servicios web, típicamente protegidas detrás de un cortafuegos corporativo.



Seguridad

Quizás no todos los usuarios tengan que tener acceso a toda la información. Los sistemas operativos tienen utilidades para gestionar todas estas necesidades. En la Intranet también se pueden publicar aplicaciones de red que podrán ser utilizadas por los usuarios para ejecutar procedimientos al estilo de la programación tradicional, pero con una ventaja: todo el software estará centralizado y esto facilitará su mantenimiento.



Ampliación

Los usuarios de una Intranet no tienen por qué estar aislados; es posible definir para ellos accesos a Internet de modo que les sea transparente si un servicio está dentro o fuera de su propia red de área local.

En corporaciones con delegaciones distribuidas geográficamente en puntos alejados, el acceso desde la red de área local de una de las delegaciones hasta los servicios de otra se puede realizar a través de Internet de modo transparente, e incluso utilizando los mismos protocolos de la LAN mediante la creación de túneles de protocolos y tecnologías de redes privadas virtuales (VPN).

Para posibilitar el acceso a Internet de toda una LAN es necesaria una conexión a Internet a través de un encaminador IP que gestione las conexiones TCP/IP desde dentro de la LAN hasta el exterior o viceversa. Para realizar esta conexión también podemos utilizar los servicios de un servidor proxy o la técnica de enmascaramiento IP, a los que nos referiremos próximamente.

Extranet es una red virtual que invoca las tecnologías Internet como si fuera una Intranet extendida más allá de los límites geográficos de la empresa. Por ejemplo, se puede construir una Extranet utilizando tecnologías para la creación de redes privadas virtuales (VPN), que es un modo de simular accesos a redes locales utilizando redes públicas, y así proporcionar acceso a algunos de los datos internos de la Intranet propia a los clientes o proveedores que lo necesiten para sus relaciones comerciales con la propietaria de la Extranet. El acceso a la Intranet se haría a través de Internet, es decir, el túnel generado por la VPN residiría en Internet. La Extranet es el ejemplo más completo de integración de los tres modelos de redes basados en IP.



Ampliación

Las herramientas de **groupware** no se limitan solo a soluciones de escritorio. Las más eficaces son las que están centralizadas. Las soluciones de mensajería electrónica en servidor integran muchos componentes orientados a dar servicios de colaboración. Las compañías que sirven software ofimático están haciendo evolucionar sus aplicaciones comerciales, convirtiéndolas en utilidades aptas para el trabajo en grupo e integrando todo lo que un puesto de trabajo puede necesitar a través de medios electrónicos de colaboración.



CEO

S M R _ R L _ A A b a d _ 0 4 _ ConfigMailMarshal.docx
Documento que contiene información sobre configuración de un servidor de correo electrónico (MailMarshal).

3.2. Servicios de comunicación personal y relacional

Es muy probable que el correo electrónico sea el servicio proporcionado por Internet de mayor difusión después de la web. Esto hace que el estudio de la tecnología de mensajería electrónica, en todas sus manifestaciones, tenga una importancia especial que intentaremos cubrir seguidamente.

A. Herramientas colaborativas o groupware

Una de las aplicaciones más interesantes que se pueden establecer en redes corporativas es el llamado software colaborativo o herramientas **groupware**. Fundamentalmente, estas aplicaciones consisten en una serie de módulos de software integrados entre sí en el ámbito de una red, que permiten el trabajo en equipo de los participantes en un proyecto. La herramienta de groupware más básica es el correo electrónico. No obstante, se ha observado en estos últimos años una sofisticación importante de los programas de colaboración en grupo: pizarra electrónica compartida, transferencia de ficheros, uso compartido de programas, conversación electrónica, audioconferencia y videoconferencia, etc.

B. Servidores de correo

El protocolo más extendido para el servicio mail de Internet es **SMTP** (*Simple Mail Transfer Protocol*). Los mensajes electrónicos confeccionados según las normas de SMTP solo pueden contener caracteres ASCII de 7 bits, es decir, ni siquiera se permiten caracteres acentuados o especiales. Tampoco permite la transferencia de ficheros binarios, por lo que este sistema de correo electrónico está muy limitado. Para salvar estas limitaciones, se incorporó a SMTP la codificación UUENCODE que permite solucionar estos inconvenientes.

Otro estándar muy utilizado que está desplazando a los demás es **MIME** (*Multipurpose Internet Mail Extension*), que permite incluir en el mensaje de correo cualquier información binaria: voz, vídeo, imagen, etc.



Ampliación

Fundamentalmente **SMTP** se encarga de transferir correo electrónico entre distintos servidores y de mover mensajes desde los clientes a los servidores; por ello necesita complementarse con otros protocolos que descarguen el correo recibido desde los servidores a las aplicaciones clientes. Entre estos protocolos se encuentran **POP** (*Post Office Protocol*, Protocolo de oficina de correos) e **IMAP** (*Internet Message Access Protocol*, Protocolo Internet de acceso a mensajes), aunque en sistemas más sofisticados se puede utilizar **RPC** (*Remote Procedure Call*, Llamada a procedimiento remoto) como aplicación cliente-servidor. Actualmente uno de los métodos más usados para el acceso al

correo electrónico es hacer que el cliente sea el propio explorador de Internet que accederá al buzón apropiado a través de su URL.

Actualmente se están utilizando con mucha frecuencia unos protocolos semejantes a los descritos aquí, pero con conexiones cifradas. De este modo, aunque se produjeran escuchas en la red, el atacante o usurpador de la información no podrá descifrar su contenido garantizando así la privacidad de las comunicaciones. Por ejemplo, SMTP está siendo sustituido por SMTPS (SMTP seguro), IMAP por IMAPS (IMAP seguro), etc.



Investigación

En la dirección <http://mxtoolbox.com/blacklists.aspx> tienes una página web que admite como argumento un nombre de dominio de correo electrónico, es decir, la parte de la dirección de correo electrónico que se escribe a la derecha del símbolo @. Escoge un grupo de direcciones electrónicas con diferente dominio y prueba si están dadas o no de alta en alguna lista negra de spam. Busca por tu cuenta otras páginas sobre *blacklist* y repite la comprobación.

Para poder acceder al servicio de correo electrónico de Internet debemos tener, además del cliente de correo (Fig. 4.17), un buzón en el servidor de algún proveedor de correo Internet. Este suele ser un servicio básico cuando se contrata una cuenta de acceso a Internet, incluso aunque sea gratuita.

Actualmente la mayor parte de los usuarios utilizan clientes de correo electrónico web que no requieren instalación en los equipos porque permiten gestionar el correo desde el navegador de Internet.

Los servidores de correo suelen utilizar el puerto 25, que es el puerto utilizado por SMTP, para intercambiar correos con otros servidores. La capacidad de envío y recepción se puede restringir mediante algún método de autenticación; no obstante, si queremos recibir correos de cualquier persona deberemos dejar abierta la autenticación anónima de modo que quien quiera comunicar con el servidor pueda hacerlo sin necesidad de conocer ninguna contraseña.

Una extensión de los sistemas de correo son los sistemas de mensajería instantánea que forman grandes redes de usuarios y que simulan el sistema de mensajería telefónica SMS.



Vocabulario

Blacklist o lista negra: es una base de datos que contiene referencias a sitios web, direcciones o dominios de correo electrónico, direcciones IP, etc. desde los que se llevan a cabo acciones delictivas o que presentan problemas de seguridad como virus, correo spam, etc. Los administradores de red consultan estas *blacklists* para impedir conexiones a sus sistemas desde estas direcciones con objeto de protegerlos.

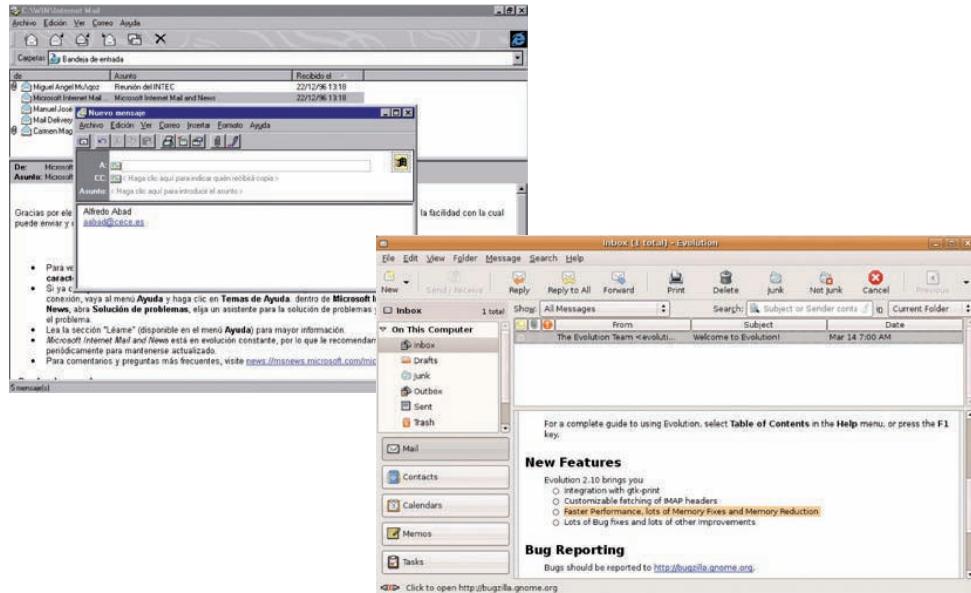


Fig. 4.17. Cliente de correo electrónico para Internet y confección de un nuevo mensaje con Outlook Express (izquierda) y cliente de correo electrónico de software libre (Evolution) para Linux (derecha).

En la Fig. 4.18 hay una representación de la consola de administración de Microsoft Exchange Server, sistema de correo electrónico que utiliza el Directorio Activo de Microsoft como servicio de directorio de buzones. También podemos ver los almacenes de datos (buzones y carpetas públicas), los protocolos habilitados para este servidor de correo y en especial el servidor SMTP con las colas de entrega de mensajes que tiene pendientes en ese momento.

En primer plano se describe la configuración del conector SMTP de Internet, que es el componente de software que utilizará el servidor SMTP para entregar correo al exterior. Por último, se especifica que el servidor utilizará un servidor DNS para averiguar dónde entregar cada correo.

En la Fig. 4.19 podemos contemplar dos fichas correspondientes a la configuración del servidor SMTP.

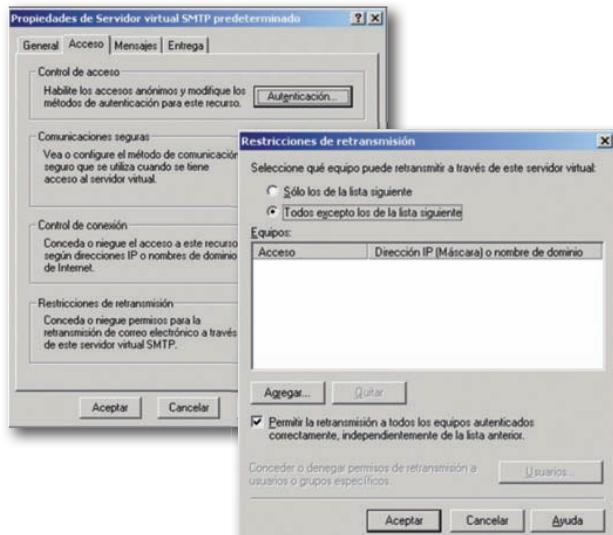


Fig. 4.19. Algunos detalles de las fichas de configuración del servidor SMTP para Microsoft Exchange Server, el servidor de correo electrónico empresarial de Microsoft.

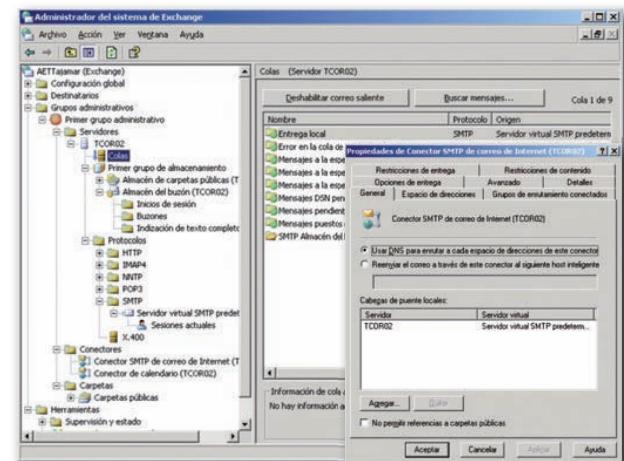


Fig. 4.18. Consola de administración de Microsoft Exchange Server.

En la figura aparecen parámetros relativos a la autenticación de los usuarios, si se utilizará un certificado digital para la realización de conexiones seguras, quiénes podrán conectarse al servidor (por ejemplo, se pueden restringir las conexiones a algunas direcciones IP, o a algunos dominios) y, por último, si se podrá hacer o no **relay** (distribuir mensajes hacia otros servidores de correo electrónico).

Vemos que solo se puede hacer relay con los mensajes procedentes de equipos que hayan sido correctamente autenticados; por tanto, un intruso solo podrá hacer **spam** si conoce una cuenta de ese directorio activo que tenga derechos de acceso al servidor SMTP.

La parte más crítica de configuración de un servidor de correo electrónico se refiere a las retransmisiones de correo puesto que, si no se hace bien, el servidor quedará expuesto para que se pueda utilizar indebidamente como servidor de correo spam.



Actividades

7. Comprueba si son ciertos o falsos los siguientes enunciados:
 - a) Una Intranet es una red local que utiliza tecnología Internet para brindar sus servicios de red.
 - b) Una Intranet y un Extranet solo se diferencian en el tamaño de la red.
 - c) Los servidores de correo electrónico utilizan los protocolos http y ftp para el intercambio de mensajes de correo.
 - d) MIME es un protocolo utilizado en la codificación de mensajes electrónicos.
 - e) El puerto estándar habitual para el intercambio de mensajes entre servidores de correo electrónico es el 125.
8. Déjate guiar por las ayudas electrónicas de algunos clientes de correo electrónico (por ejemplo: Outlook y Evolution) para configurar sobre ellos el acceso como cliente a una cuenta de correo electrónico. Prueba a utilizar —si el servidor de correo lo permite— varios protocolos: POP3, IMAP, MAPI y http.
9. Descarga de <http://www.marshall.com/> o en <http://www.m86security.com/> una versión de prueba de MailMarshal y sigue las instrucciones de la documentación para instalar un servidor de correo electrónico con capacidad antispam. Posteriormente crea algunas cuentas de correo electrónico locales para algunos usuarios. Despues abre una sesión en diversos clientes Windows y Linux y comprueba que pueden enviar y recibir correo electrónico.

A**Vocabulario**

Backbone: segmento de red de alta velocidad que hace las funciones de nervio central de una red local. En cableado estructurado el backbone suele conectar los commutadores de planta en un edificio, o distintos edificios en una red de campus. En general, debe tomarse por *backbone* un canal de alta velocidad que conecta otros elementos secundarios.

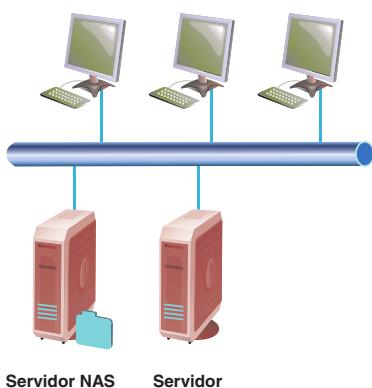


Fig. 4.20. Almacenamiento NAS.

Ampliación

Hay, por tanto, dos redes en una SAN: 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 conectan todos los medios de almacenamiento. Los entornos en que está indicada una solución SAN son aquellos en que los backups son críticos, en los clusters de alta disponibilidad, en las aplicaciones con bases de datos de gran volumen, etc.

A**Vocabulario**

SAN: es una red especializada en conectar virtualmente un conjunto de discos a los servidores que los utilizarán con tecnologías de alta velocidad y, frecuentemente, redundantes.

4. Sistemas de almacenamiento en red

Es frecuente que el volumen de datos a los que se tenga que acceder a través de 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 corresponden a su vez con otras tantas 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.
- **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.
- **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.

Los equipos SAN más modernos pueden alcanzar velocidades de transmisión de datos desde los discos de varios Gbps (véase Fig. 4.21).

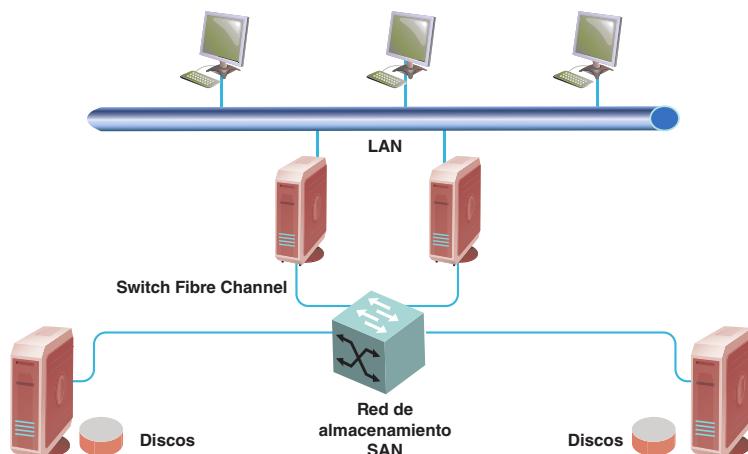


Fig. 4.21. Modelo de almacenamiento SAN.

Los switches de una red SAN suelen utilizar la tecnología Fibre Channel y frecuentemente están duplicados para garantizar el servicio. Emergentemente 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. La proliferación de software libre ha hecho que en muchas instalaciones se esté utilizando software servidor bajo licencia GPL, típicamente sistemas operativos de tipo Linux. Una plataforma que está creciendo espectacularmente debido a que su coste es nulo es Samba, que es una implementación del protocolo SMB/CIFS (CIFS es el nombre del protocolo SMB en la implementación moderna de Microsoft) bajo licencia GNU para el

acceso por red a los sistemas de ficheros de Microsoft Windows, que es el equivalente Linux del protocolo SMB/NetBeui de Microsoft.

En Samba deben configurarse la parte de servidor (en servidores) y la parte de cliente en todos los equipos que necesiten conectarse a unidades remotas servidas con SMB. Las estaciones Windows no necesitan la instalación de cliente ya que es un protocolo natural en ellas que viene habilitado por defecto al configurar las tarjetas de red.

En el mundo UNIX y Linux se utiliza mucho el protocolo **NFS** (*Network File System*, Sistema de ficheros de red), semejante —aunque no equivalente ni compatible— a Samba. Existe software en el mercado para que los sistemas Windows también puedan acceder o brindar sus discos mediante NFS.

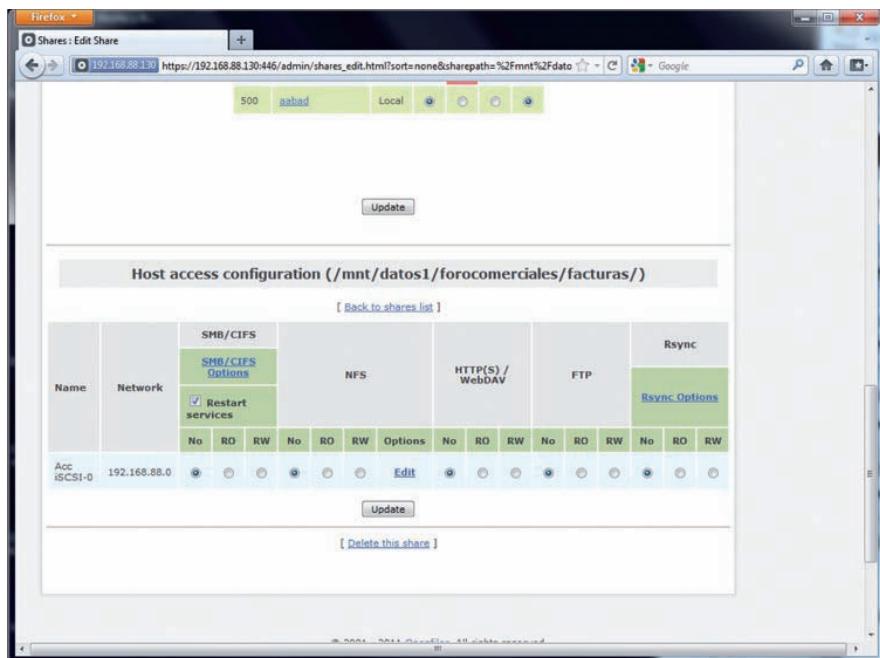


Fig. 4.22. Página web de gestión de las unidades de red compartidas bajo diversos protocolos en Openfiler, una distribución Linux que gestiona servicios de disco mediante SMB/CIFS, NFS y otros protocolos de red.

Ejemplos

Samba es una tecnología GNU que permite utilizar servidores de discos e impresoras de Microsoft desde clientes Linux. También pueden instalarse servidores Samba sobre Linux para que los discos compartidos por Samba puedan ser utilizados a través de la red por cualquier sistema operativo sobre el que corra el cliente Samba. Fundamentalmente se trata de que los clientes Linux puedan ejecutar la pila de protocolos de Microsoft para servirse de los servicios de discos de esta compañía, de modo que Samba se convierte en el software de Microsoft para Linux.

Existen muchas implementaciones de la tecnología Samba, por eso cada distribución de Linux se configurará de un modo distinto. En el ejemplo de la Fig. 4.23 podemos ver un configurador gráfico. En la ficha «Server settings» se configuran los parámetros de red. En la de «Users» se pueden dar de alta los usuarios del servicio. En la de «Shares» se darán de alta todas las carpetas o discos que queramos compartir en la red.

A

Vocabulario

Samba: es una implementación del protocolo de presentación SMB/CIFS bajo licencia GNU para el acceso por red a los sistemas de ficheros de Microsoft Windows.

En la Fig. 4.24 se puede ver un sencillo modo de compartir impresoras en Ubuntu utilizando Samba como servicio servidor sobre SMB/CIFS. Se puede apreciar una impresora local denominada Deskjet-3840 que es compartida en la ventana de opciones de servidor mediante el marcado de la publicación de impresoras. A partir de ese momento, las otras estaciones de la red que puedan explorar los recursos de la red podrán ver la impresora compartida en este equipo y podrán conectarse desde la ubicación remota a ella, si tienen los permisos adecuados para poder utilizarla, como si dispusieran de ella en local.

En el servidor:

- Nombre NetBIOS: es el nombre, según la tecnología Microsoft, que tomará el nodo Linux para ser utilizado desde la interfaz NetBIOS.
- Los servicios tienen restricciones de usuario: los usuarios deberán tener cuenta en el servidor Linux para poder acceder a los recursos compartidos.
- Redes y hosts a los que se les permite la conexión: solo los host y redes que poseen las direcciones que se especifican podrán conectarse al servicio.

En el cliente:

- URL de conexión: es un protocolo smb (réplica del utilizado por Microsoft). Se especifican el nombre de usuario, la dirección IP (o nombre) del servidor Samba y el nombre de la carpeta a la que nos queremos conectar y que previamente ha tenido que ser compartida en el servidor.

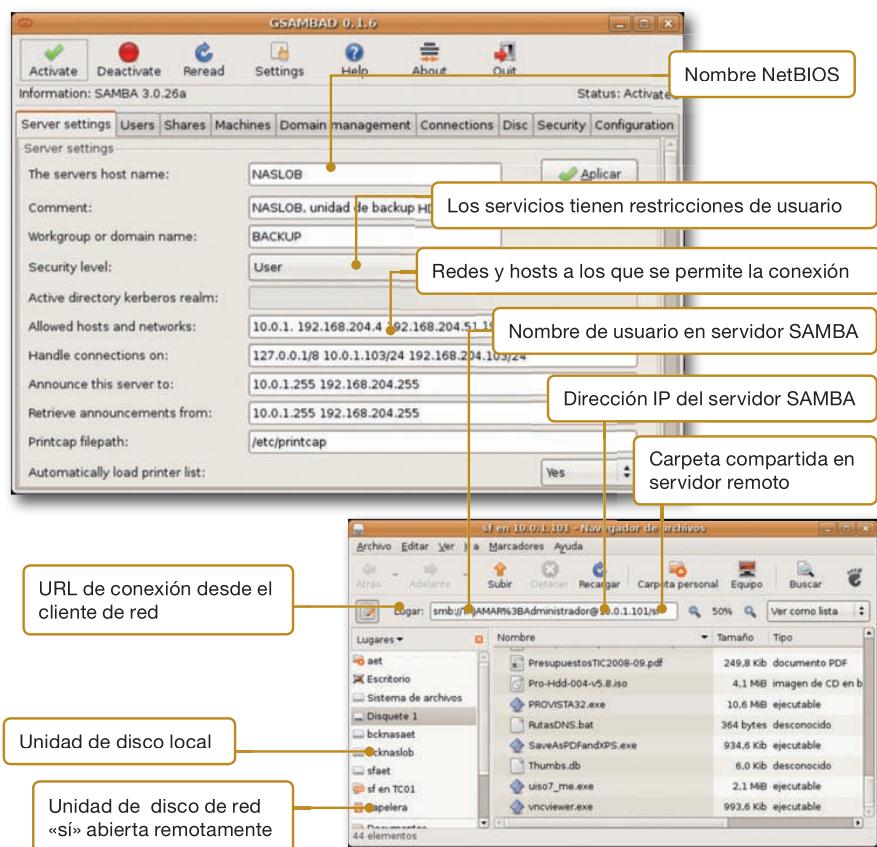


Fig. 4.23. Consola de configuración de un servidor Samba sobre Linux (a la izquierda) y apertura de una unidad de red Windows mediante un cliente Samba de Linux (a la derecha).

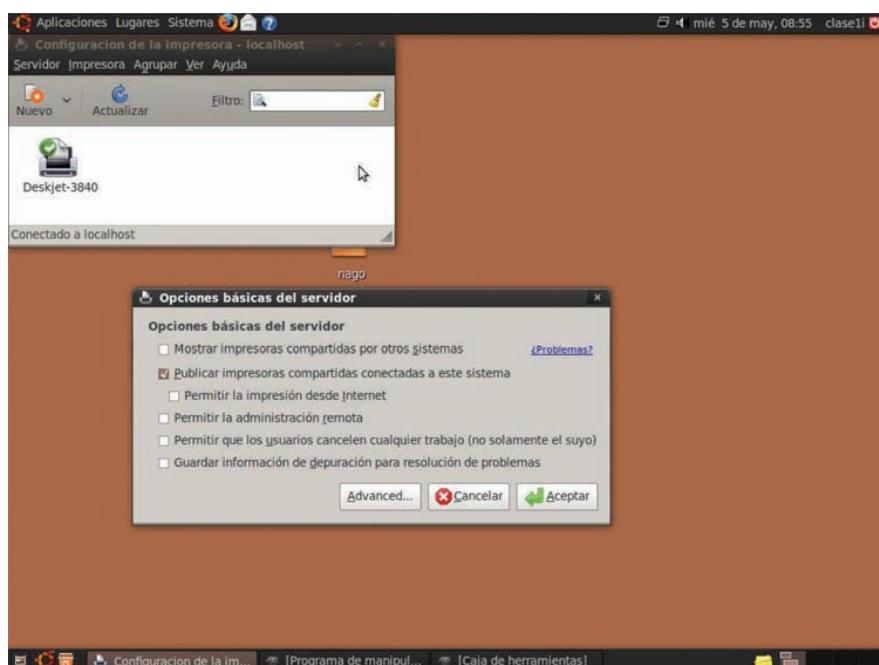
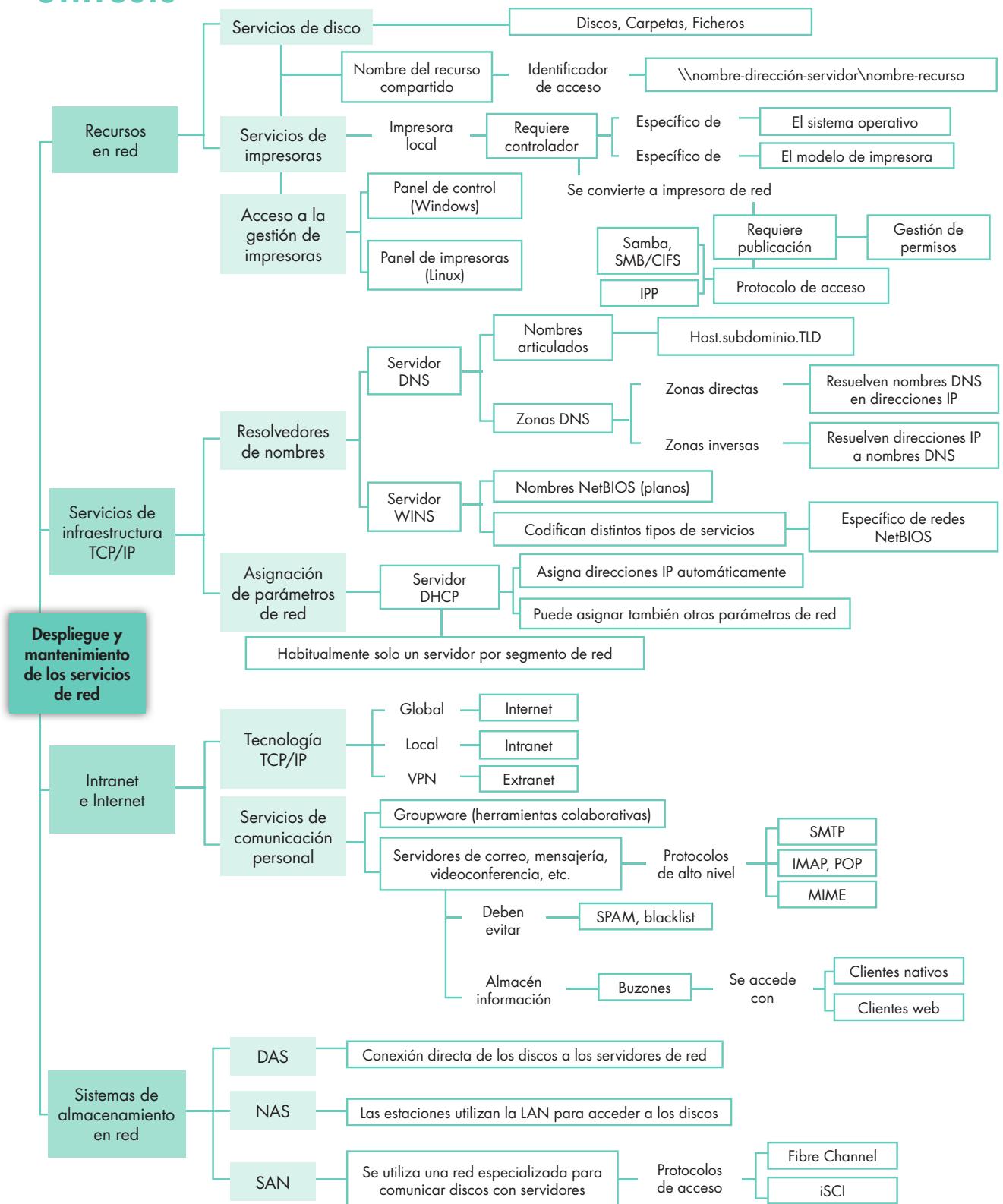


Fig. 4.24. Publicación de una impresora local en una estación Ubuntu mediante Samba.

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de las distintas tecnologías de compartición de recursos en la red:

a) Discos, carpetas	1) Samba
b) Impresoras	2) Fibre Channel
	3) iSCSI
	4) SMB/CIFS
	5) NFS
	6) IPP

2. El controlador de un dispositivo de impresora...

- a) Es específico para cada sistema operativo.
- b) Es específico para cada modelo de impresora.
- c) Es específico para cada sistema operativo y para cada modelo de impresora.
- d) Es común a todos los sistemas operativos, pero distinto para cada modelo de impresora.

3. Asocia las siguientes funciones a los diferentes tipos de servicios que proveen:

a) DNS	1) Resuelve nombres NetBIOS a direcciones IP
b) WINS	2) Resuelve nombres de dominio a direcciones IP
c) DHCP	3) Resuelve direcciones IP a nombres de dominio
	4) Asigna direcciones IP automáticamente

4. Los nombres de dominio DNS...

- a) Son articulados.
- b) Siempre se escriben en mayúsculas.
- c) No pueden tener más que dos puntos en su descripción completa.
- d) Se configuran en los servidores DNS.

5. Asocia las siguientes tecnologías:

a) Herramientas colaborativas	1) Groupware
b) Protocolos de correo electrónico	2) IMAP
c) SPAM	3) Blacklist
	4) POP

6. ¿Qué tecnología de las siguientes no es específica de las Intranets?

- a) Alimentación eléctrica redundante.
- b) Servidor de correo electrónico.
- c) Servidor web.
- d) Red de área local.

7. La tecnología iSCSI utiliza:

- a) Discos de alta velocidad.
- b) Discos de baja velocidad.
- c) Protocolos de la pila TCP/IP para encapsular el protocolo SCSI de acceso a discos.
- d) Protocolo NetBIOS para nombrar los discos de la red.

8. Enlaza los siguientes elementos característicos de distintos tipos de almacenamiento en red:

a) DAS	1) Se crea una red específica para el acceso al almacenamiento
b) NAS	2) Los discos se conectan a la red
c) SAN	3) Los discos se conectan directamente al servidor

9. Enlaza los siguientes elementos característicos sobre distintos modelos de redes TCP/IP:

a) Internet	1) Red globalizada
b) Intranet	2) Conexión a la Intranet de otra organización
c) Extranet	3) Tecnología Internet dentro de una corporación

10. En una red de área local:

- a) Únicamente debe haber un servidor DHCP por cada segmento de la red.
- b) Debe haber un servidor DHCP por cada router ADSL.
- c) Hay que instalar necesariamente un servidor DHCP para que la LAN funcione correctamente.
- d) El servidor DHCP asigna direcciones IP automáticamente, además de otros parámetros de la red.

Solución: 1: a-(1, 2, 3, 4 y 5), b-(1 y 6); 2: son verdaderas la a y la b; 3: a-(2 y 4), b-a, c-4; 4: son verdaderas la a y la d; 5: a-1, b-(2 y 4), c-3; 6: a; 7: c; 8: a-3, b-2, c-1, 9: a-1, b-3, c-2; 10: a y d.



Comprueba tu aprendizaje

I. Configurar los servicios básicos de discos e impresoras compartidos en la red

1. Un servidor comparte una impresora en la red. El administrador del sistema ha limitado el uso de la impresora a algunos usuarios concretos, denegándose al resto. Un cliente de red intenta conectarse a la impresora de red compartida por el servidor y, al realizar la conexión, el servidor le presenta una ventana para que se autentifique con un nombre de usuario y contraseña válidos. El cliente tiene localmente un conjunto de cuentas de usuario con sus contraseñas y el servidor tiene las suyas.

- a) El permiso de imprimir de la impresora en el servidor, ¿debe hacerse sobre un usuario del servidor o del cliente?
- b) Si la cuenta utilizada en el cliente coincide con una cuenta en el servidor y las contraseñas son idénticas, ¿podrá imprimir el cliente?
- c) ¿Qué pasaría si coinciden en el cliente y en el servidor el nombre de usuario, pero no sus contraseñas?

2. Localiza en la red los lugares en donde haya información de interés para los usuarios de la red y comparte las carpetas en la red de modo que desde cualquier estación se puedan realizar conexiones contra esas carpetas compartidas. La información que se compartirá puede estar tanto en servidores como en estaciones cliente.

Deberás tener cuidado con la asignación de permisos para no tener problemas de pérdidas de información o de intrusismo.

Por último, elabora una guía de recursos de ficheros compartidos que pueda ser útil al resto de los usuarios de la red como potenciales clientes de esta guía de recursos.

3. Localiza las impresoras de los equipos conectados en la red y compártelas con el resto de usuarios de la red. Deberás asignar los permisos adecuados para que cada usuario tenga acceso a algunas impresoras, aunque no necesariamente a todas.

Publica una guía de recursos de impresión para repartir entre los usuarios de la red.

II. Gestionar el acceso a los servicios de infraestructura de redes IP

4. Una red tiene desplegados varios servicios de infraestructura IP para la asignación de direcciones IP y resolución de nombres. Un cliente de red tiene configurada su red de modo que sus parámetros básicos de red deben ser solicitados a un servidor DHCP.

a) ¿Qué debe hacerse en el cliente para que tome sus parámetros correctos del servidor DHCP?

b) ¿Qué debe hacerse en el servidor para que admita clientes DHCP?

c) ¿Puede el servidor DHCP asignar al cliente DHCP las direcciones de sus revolvedores de nombres DNS y WINS?

d) ¿Cuándo utilizarías DNS y cuándo WINS?

5. Sobre la instalación de un sistema operativo Windows Server o Linux, instala el software de servidor DNS (bind9 en Linux).

a) Sigue la ayuda gráfica si elegiste Windows o la orden «man» si elegiste Linux para configurar un sistema básico con una zona DNS.

b) Crea varios registros de tipo «A» para dar de alta algunas estaciones de la red.

c) Crea un registro «MX» que asocie el dominio de correo electrónico identificado por la zona DNS con una dirección IP en donde se podría instalar un servidor de correo electrónico para el dominio.

d) Por último, asigna unos reenviadores que gestionen las peticiones DNS en Internet.

e) Sobre una estación cliente, configura su red para que apunte al DNS recién creado y comprueba que es capaz de resolver nombres DNS de máquinas locales y de sitios Internet.

6. Busca en Internet alguna empresa gestora de dominios de Internet y estudia las condiciones en que se pueden contratar los dominios.

Sugerencia de búsqueda: <http://www.dyndns.com/>

III. Utilizar la tecnología IP para montar servicios de colaboración entre usuarios

7. Una red de área local alberga, entre otros servicios, un servidor de correo electrónico que ofrece mensajería electrónica a los buzones de los usuarios identificados por un dominio de correo que coincide con su zona DNS. Supongamos que el nombre de esta zona fuera «oficina.lab» y que, por tanto, los usuarios de la red tuvieran direcciones electrónicas del estilo **usuario@oficina.lab**.

a) ¿Pueden estas direcciones de correo utilizarse fuera de la red de área local? ¿Por qué?

b) Si la empresa tiene contratado el dominio **oficina.es**, ¿podrían ahora utilizarse las direcciones **usuario@oficina.es** en Internet?

Comprueba tu aprendizaje

- c) ¿Hay que configurar algún parámetro especial en la tarjeta de red de los clientes para que estos puedan enviar correo electrónico? ¿Y en el programa cliente de correo electrónico, por ejemplo, en Outlook?
- d) ¿Cómo sabría el servidor de correo electrónico de nuestro buzón a qué servidor debe enviar un correo para que alcance su destino?
8. En la siguiente tabla encontrarás tres columnas. Las dos primeras contienen servicios, elementos de configuración o, en general, ámbitos de relación. En la tercera deberás escribir cuál es el elemento que relaciona la primera columna con la segunda. Por ejemplo, en la primera fila, que se toma como modelo, se indica que lo que relaciona los nombres DNS con las direcciones IP es el servicio DNS.

Lo que relaciona:	Con:	Es:
Nombres DNS	Direcciones IP	Servidor DNS
Nombres NetBIOS	Direcciones IP	
Registro MX	DNS	
Servidor DHCP	Cliente DHCP	
Samba	Linux	
IPP	Internet	
Ámbito de red	IP y máscara de red	
iSCSI	Discos	
Puerto 25	Correo electrónico	

9. Explica cuáles podrían ser las causas de error y por dónde empezarías a investigar en las siguientes situaciones en las que se produce un mal funcionamiento de la red:

- a) Cuando un cliente de la red arranca no obtiene la dirección IP esperada.
- b) El cliente tiene una dirección IP correcta, pero no puede hacer ping a otra máquina local por su nombre NetBIOS.
- c) El cliente puede hacer ping a otra máquina local utilizando el nombre NetBIOS, pero no su nombre DNS.
- d) Se puede hacer un ping mediante nombre DNS a otra máquina local, pero no a una máquina en Internet.
Sin embargo, sí funciona un ping a una máquina externa mediante su dirección IP de Internet.
- e) Igual que en el caso anterior, pero tampoco funciona el ping a máquina externa con dirección IP de Internet.
- f) Arrancamos dos clientes de red que obtienen su dirección mediante DHCP y el primero obtiene una dirección en la red 192.168.1, mientras que el segundo la obtiene en la red 192.168.2.
Como la máscara asignada es 255.255.255.0 no tienen comunicación entre ellos y pierden la comunicación entre sí.
- g) Encendemos una máquina y nos dice que su dirección IP ya existe en la red (está duplicada).
- h) Un cliente tiene por nombre CLIENTE, su nombre de dominio es laboratorio.lab y su dirección IP es 192.168.1.1.
Sin embargo, cuando otro cliente de la red hace ping contra CLIENTE.laboratorio.lab, el nombre se resuelve como 192.168.1.12.
Como esta dirección no existe en la red, el ping falla, sin embargo ping contra 192.168.1.1 funciona correctamente.



Práctica final

MUY IMPORTANTE:

Esta realización práctica exige haber efectuado previamente las dos actividades siguientes:

1. Haber comprendido bien los contenidos de las unidades 1 a 4 que constituyen los dos primeros bloques temáticos del libro.
2. Haber leído y comprendido el epígrafe 1 de la unidad final 9, en donde se describe el proyecto, junto con la práctica de final del bloque 1.

En esta práctica de final de bloque intentaremos conseguir los siguientes objetivos:

- Decidiremos la configuración de red de los equipos.
- Crearemos los servicios básicos de infraestructura de red.
- Estableceremos los servicios de impresión.
- Compartiremos las carpetas de fondos bibliográficos en la red.

Hemos hecho las siguientes asignaciones:

- Los servidores y enrutador tienen unas direcciones estáticas muy concretas.
- Los clientes fijos, sean Windows o Linux, tienen dirección estática. Todos están en la red 192.168.1, pero en planta baja se han asignado del 21 al 26 y en la planta alta del 31 al 33. Quedan huecos de direcciones IP sin utilizar, pero esto no importa para la instalación.
- Los equipos especiales (impresoras, comutadores, punto de acceso y videocámara) tienen direcciones

1. Identificación de las redes y equipos

La solución aportada por el proyecto se resuelve en dos redes:

- Una red de área local, que en adelante denominaremos LAN.
- Una red de área extensa, que denominaremos WAN, que representa la conexión a Internet a través del cortafuegos/proxy.

En la LAN se integran todos los equipos informáticos e impresoras, incluido el cortafuegos (en su interfaz interna), la videocámara y el punto de acceso.

A la WAN pertenecen en enrutador ADSL y el cortafuegos (en su interfaz externa).

Para que todos los equipos de la LAN puedan comunicarse entre sí sin necesidad de dispositivos externos a la LAN (por ejemplo, un encaminador interno), es necesario que su espacio de direccionamiento IP sea compatible.

Elegiremos las direcciones de la red 192.168.1 como el espacio propio de la LAN y las direcciones 10.1.1 como espacio de red de la WAN.

Ahora vamos a asignar nombres y direcciones a cada equipo de la red (Tabla 1).

41 a 46 y puede que no necesiten la puerta por defecto ya que serán dispositivos que no precisarán acceso a Internet.

- Todos los portátiles, que serán clientes móviles, solicitarán a un servidor DHCP una dirección dinámica, que estará comprendida entre 102.168.1.51 y 192.168.1.70: se podrán conectar, por tanto, un máximo de 20 equipos portátiles.
- Todos los equipos (salvo el router) configurarán su DNS apuntando a 192.168.1.10 que es donde disponemos de un servidor DNS.

Práctica final

Nombre equipo	Tipo de equipo	IP	Máscara	Ruta por defecto	Observaciones
SRV	Servidor Windows Server 2008	192.168.1.10	255.255.255.0	192.168.1.100	La puerta por defecto apunta a la interfaz interna del cortafuegos (192.168.1.100).
Ipcop	Cortafuegos/proxy Linux	Interna: 192.168.1.100 Externa: 10.1.1.100	Interna: 255.255.255.0 Externa: 255.255.255.0	10.1.1.1	Puerta por defecto de ipcop dirigido al encaminador ADSL.
PCB1	Cliente fijo Windows	192.168.1.21	255.255.255.0	192.168.1.100	
PCB2	Cliente fijo Linux	192.168.1.22	255.255.255.0	192.168.1.100	
PCB3	Cliente fijo Linux	192.168.1.23	255.255.255.0	192.168.1.100	
PCB4	Cliente fijo Windows	192.168.1.24	255.255.255.0	192.168.1.100	
PCB5	Cliente fijo Windows	192.168.1.25	255.255.255.0	192.168.1.100	
PCB6	Cliente fijo Windows	192.168.1.26	255.255.255.0	192.168.1.100	
ImpreB1	Impresora red	192.168.1.41	255.255.255.0	192.168.1.100	
ImpreB2	Impresora local				No tiene parámetros de red de nivel 3.
PCA1	Cliente fijo Windows	192.168.1.31	255.255.255.0	192.168.1.100	
PCA2	Cliente fijo Windows	192.168.1.32	255.255.255.0	192.168.1.100	
PCA3	Cliente fijo Linux	192.168.1.33	255.255.255.0	192.168.1.100	
ImpreA1	Impresora red	192.168.1.42	255.255.255.0	192.168.1.100	
AP1	Punto de acceso Wi-Fi	192.168.1.43	255.255.255.0		
VC1	Videocámara IP	192.168.1.44	255.255.255.0		
Eth1	Conmutador Ethernet	192.168.1.45	255.255.255.0		Conmutador de planta baja.
Eth2	Conmutador Ethernet	192.168.1.46	255.255.255.0		Conmutador de planta alta.
Router1	Encaminador ADSL	Interna: 10.1.1.1 Externa: DHCP proveedor	Interna: 255.255.255.0 Externa: proveedor	La asignará el proveedor.	La IP externa y la ruta por defecto deben ser asignadas por el proveedor de Internet.
SERVICIO DHCP	Clientes inalámbricos móviles	192.168.1.51 a 192.168.1.70	255.255.255.0	No se asignará.	Asignados por DHCP.

Tabla 1. Descripción de los equipos con su direccionamiento IP de toda la instalación.



Práctica final

2. Identificación de los servicios de red

Ahora vamos a concretar los servicios de red que serán necesarios para resolver la instalación. Los dividiremos en servicios de infraestructura de red y en servicios de usuario.

Los servicios de infraestructura de red básicos serán:

- **Servidor DNS:** en donde se registrarán todos los nodos de la red.
- **Servidor DHCP:** que asignará las direcciones IP dinámicamente a los clientes inalámbricos.
- **Servicio de directorio:** habrá que crear algunas cuentas en los equipos para que se puedan identificar algunos usuarios.

Los servicios de usuarios básicos serán los siguientes:

- Servicio de compartición de carpeta de fondos editoriales.
- Servicios de impresión.
- Servicio de acceso a Internet (lo dejaremos para más adelante).

Todos los servicios serán proporcionados por el servidor SRV, excepto el acceso a Internet, de cuyo servicio se encargará el cortafuegos/proxy.

3. Operaciones en los servidores

PHES recibe los equipos con el software preinstalado, pero sin configurar. Para ello, en sus instalaciones, una vez recibidos los equipos, los desempaquetará y monta una red de laboratorio en la que irá configurándolos uno a uno según los datos de red expuestos anteriormente.

Lo primero que hay que hacer es instalar en el servidor SRV (Windows Server 2008) los servicios de infraestructura de red (servicios DHCP y DNS). Pero como estos servicios tienen que ser muy estables, puesto que de ellos dependerá toda la red, hay que dar al equipo servidor el nombre y configuración de red correctos.

3.1. Configuración inicial del equipo SRV

Nada más arrancar, el equipo preinstalado nos solicita que asignemos una contraseña válida a la cuenta de administrador y después nos dejará presentarnos con ella. Una vez presentados nos muestra la configuración inicial en donde el nombre del equipo es aleatorio y su configuración de red inicial está configurada como un cliente DHCP.

Procederemos a configurar el nombre del equipo (en nuestro caso SRV) y lo asignaremos a un grupo de trabajo que denominaremos CTT. Al hacer clic en el botón «Más» podremos configurar el dominio DNS que asignaremos al equipo, que en nuestro caso será *ctt.local* (un dominio que nos hemos inventado, que es interno —sin relevancia pública— y que crearemos después). Queremos que el servidor se llame *srv.ctt.local*.

Al salir de todas estas ventanas, el sistema nos dirá que necesita reiniciarse y así lo haremos (Fig. 1).

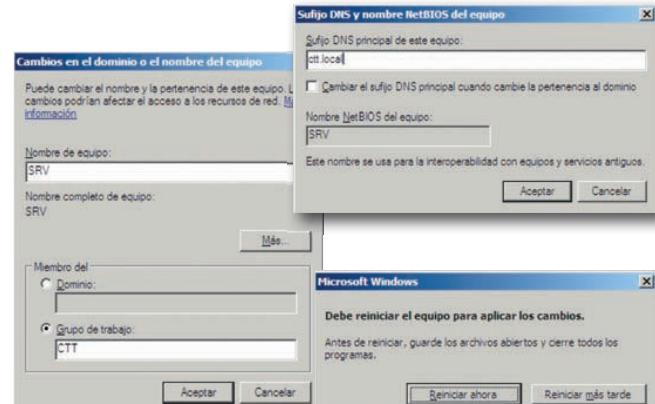


Fig. 1. Configuración del nombre del equipo, grupo de trabajo y dominio DNS.

3.2. Configuración de la tarjeta de red en SRV

El hardware de SRV lleva integrado en placa dos interfaces de red, pero nosotros solo utilizaremos una de ellas. La otra, para que no moleste, la desactivaremos.

Podemos acceder a la ficha de configuración de la interfaz de red desde la página de «Administrar conexiones de red» del panel de control del equipo.

Práctica final

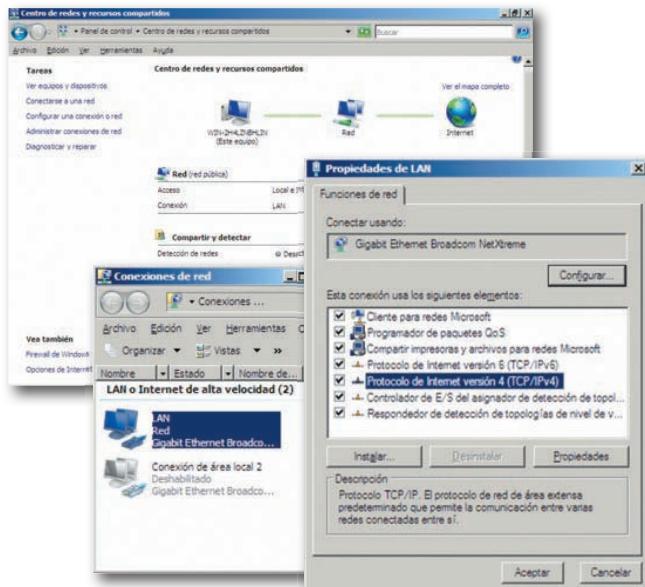


Fig. 2. Configuración de la red en la interfaz LAN.

Nosotros vamos a utilizar la tecnología IPv4, por tanto, ignoraremos las fichas de configuración IPv6, que por defecto estarán configuradas para DHCP (versión 6). Otra opción es desactivarlas.

Seleccionamos la interfaz (que hemos renombrado con el nombre de la red a la que se conecta: en nuestro caso LAN) y sacamos su ficha de propiedades (con el botón derecho del ratón). Nos movemos al elemento «Protocolo de Internet versión 4» y hacemos clic en «Propiedades» (Fig. 2).

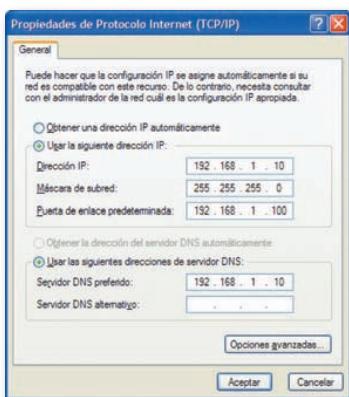


Fig. 3. Configuración de los parámetros IPv4 en la interfaz de red LAN.

En esta ficha rellenamos los campos con los datos de la tabla anterior según hemos definido en el proyecto para el servidor SRV y aceptamos (Fig. 3). Cuando finalice la operación ya tendremos configurada la red del servidor SRV.

3.3. Instalación de los servicios de infraestructura

Una vez que tenemos configurado el equipo servidor, procederemos a instalar los servicios que proveerá a la red. Partimos de la ventana inicial de administración, en la que observamos que no tiene ninguna función asignada y le pedimos que agregue funciones (servicios). Seleccionaremos los servicios que necesitamos entre todos los disponibles y aceptaremos para que el sistema proceda a instalarlos. En nuestro caso seleccionaremos los servicios de impresión, DNS y DHCP. El sistema procederá a preguntarnos por los parámetros de configuración de cada uno de los servicios.

En la configuración del DHCP crearemos un ámbito denominado «PC inalámbricos» que podrá asignar las direcciones 192.168.1.51 a 192.168.1.70 con máscara de red 255.255.255.0 a los clientes que se lo soliciten. No hemos asignado puerta de enlace predeterminada por una razón especial que comentaremos más adelante. Activamos el ámbito y aceptamos (Fig. 4).

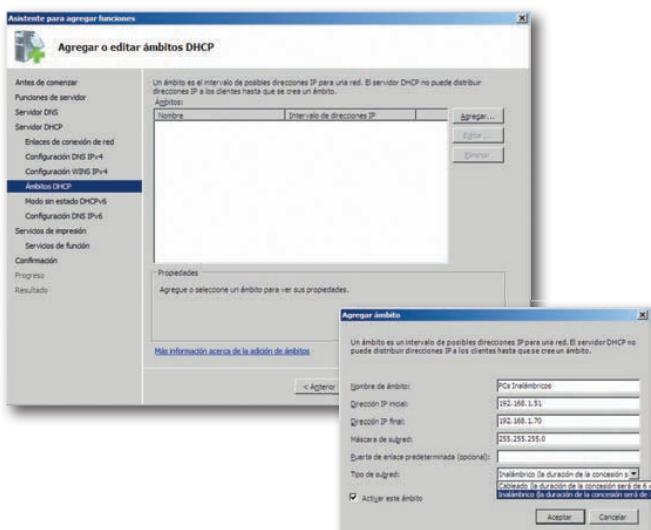


Fig. 4. Creación de un ámbito DHCP.



CEO

SMR_RL_AAbad_09_Bloque2_ConfiguracionSRV.pptx

Documento que contiene información sobre:

1. Configuración del servidor SRV.
2. Configuración de la interfaz de red de SRV.



Práctica final

El servicio DNS se configurará después de realizar la instalación. También elegimos instalar los servicios de impresión del sistema para poder compartir las impresoras en red. Como también se podrán conectar impresoras mediante IPP y estas requieren la presencia de un servidor web, el sistema instalará IIS, el servidor web de Microsoft. Ahora la ficha de administración inicial presentará las nuevas funciones que nuestro servidor ha adquirido.

3.4. Configuración del servicio DNS

Para configurar el servicio DNS arrancamos su consola de administración desde el menú de herramientas administrativas del sistema. La consola presenta las zonas de administración del DNS, que se identifican con los dominios DNS.

Nos situamos en las zonas de búsqueda directa y añadimos una zona primaria para nuestro dominio interno que es *cct.local*, que resolverá las direcciones IP de los nodos a partir de su nombre. Zona primaria significa que los datos de la zona están dentro del servidor que posee la zona. También crearemos una zona primaria inversa, que se encargará de resolver el nombre de los nodos a partir de su dirección (Fig. 5).

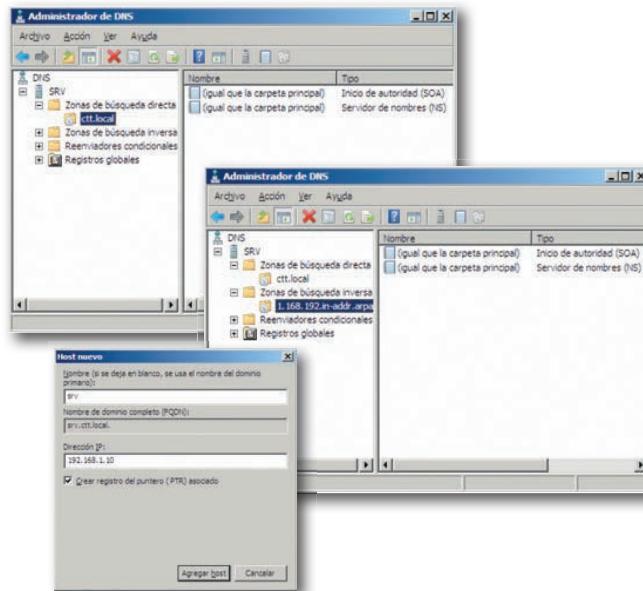


Fig. 5. Zona directa, zona inversa y alta de un nodo en el servicio DNS.

Ahora daremos de alta todos los nodos de nuestra red que vayan a estar en la zona *cct.local* mediante registros de tipo A. Después de esta operación repetitiva, el DNS queda configurado como se indica en la Fig. 6, arriba.

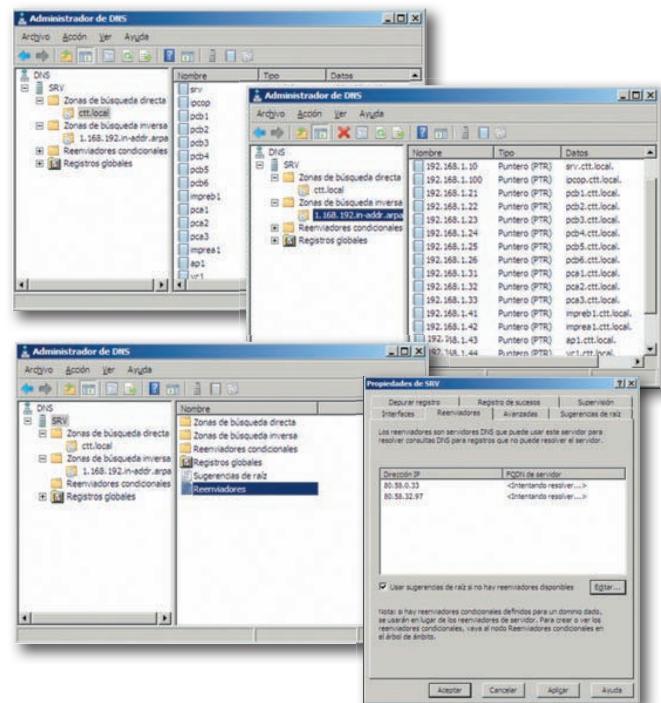


Fig. 6. Zona directa e inversa con los nodos de la LAN (arriba). Configuración de los reenviadores en el servicio DNS (abajo).

Para finalizar, daremos de alta los reenviadores, es decir las direcciones de otros servidores DNS que puedan resolver otras zonas ya que nuestro DNS, de momento, solo puede resolver los nombres del dominio *cct.local*. Rellenaremos la ficha de los reenviadores con los DNS que nos haya proporcionado nuestro proveedor de Internet (Fig. 6, abajo).

Desde este momento, cualquier cliente de la red que tenga su DNS apuntando a nuestro nuevo servicio DNS en la dirección 192.168.1.10, resolverá los nombres de la red local directamente en él y los nombres externos a la LAN a través de él utilizando los reenviadores que serán interrogados por nuestro DNS.



CEO

SMR_RL_AAbad_09_Bloque2_ServiciosInfraestructura.pptx

Documento que contiene información sobre:

1. Instalación y configuración de DHCP.
2. Instalación y configuración de los servicios de impresión.

Práctica final

4. Creación de usuarios

En cuanto a las cuentas de usuario, hay que confeccionar un sistema sencillo de directorio que sirva para restringir algunos permisos pero que permitan que los usuarios utilicen los recursos de la red de la forma más transparente posible. Puesto que la red LAN es una red mixta integrada por equipos Windows y Linux, sería muy complejo crear un dominio en un Directorio Activo de Microsoft, por lo que vamos a decidir crear cuentas locales en cada equipo: en concreto crearemos las siguientes cuentas:

- Lector (sin contraseña): será la cuenta de invitado de los lectores.
- Investigador (con contraseña): es la cuenta utilizada por los investigadores con accesos a los fondos bibliográficos propios de los investigadores.
- Bibliotecario (con contraseña): es la cuenta que utilizará el bibliotecario.

Podemos crear las cuentas desde el ícono de usuarios y grupos del panel de control o desde la correspondiente consola de administración del equipo. Añadiremos las cuentas de los usuarios citados anteriormente y saldremos de la consola (Fig. 7).

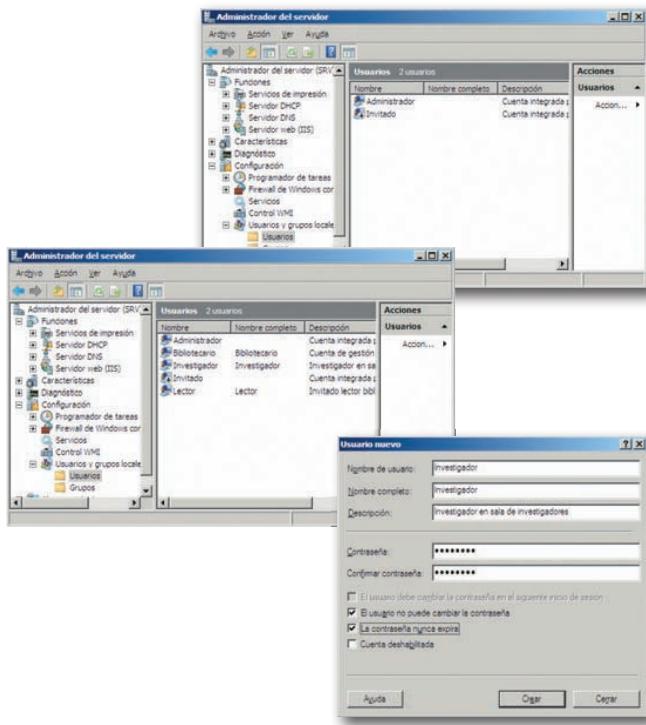


Fig. 7. Consola de administración de usuarios antes y después de la creación del usuario Investigador.

5. Impresoras

Para instalar las impresoras de la red abrimos la consola de administración de impresoras desde el menú de administración del servidor. Las impresoras de red asocian un nombre de impresora que se comparte, un controlador de impresora (software), un puerto de comunicaciones (por donde el servidor le manda los datos a la impresora) y unos permisos.

Una impresora de red se puede instalar de dos modos: haciendo que cada cliente de la red imprima directamente sobre la impresora o haciendo que en ella (a través de la red) solo imprima un servidor y que los clientes se comuniquen con este servidor cuando desean imprimir. En el primer caso tenemos una configuración p2p y en el segundo una cliente-servidor.

La primera forma tiene la ventaja de que no es necesaria la presencia del servidor para imprimir, pero, a cambio, debe crearse una cola de impresora en cada equipo de la red. Esto en nuestra red es imposible, puesto que los portátiles de los lectores móviles no los podemos gestionar nosotros.

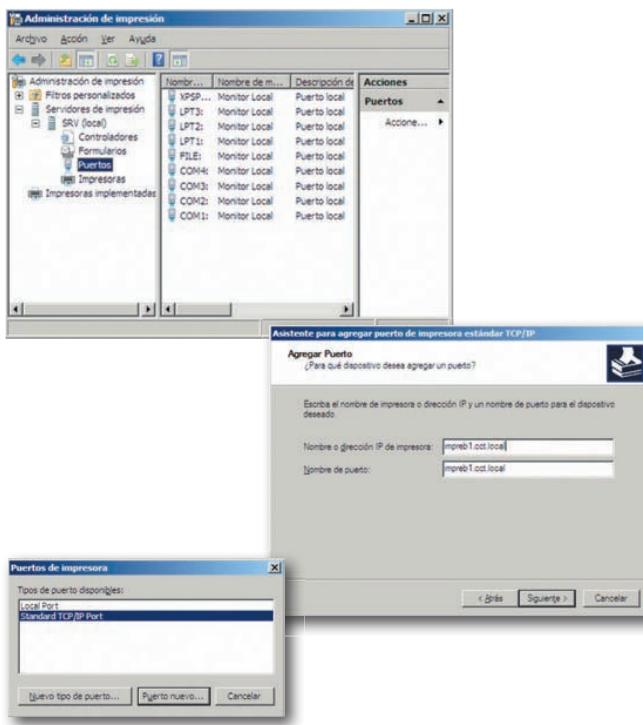


Fig. 8. Alta de un puerto de red para una impresora de red.



Práctica final

La forma cliente-servidor tiene el inconveniente de que si el servidor se estropea no se puede imprimir, pero puede centralizar todas las comunicaciones y, lo más importante: los permisos de impresión. Nosotros vamos a elegir esta segunda forma de configuración.

Además, en este modelo, una impresora local conectada al servidor (por ejemplo, por el puerto USB o por el puerto paralelo) también se podrá compartir a la red como si fuera una auténtica impresora de red: en este caso, no compartimos la impresora sino su cola de impresión.

En primer lugar, crearemos el puerto de comunicaciones por el que se van a comunicar el servidor en donde crearemos la cola de impresión y la impresora que leerá sus trabajos de esa cola. Procederemos a dar de alta un nuevo puerto TCP/IP que apunte al nombre DNS o dirección IP de la impresora de red. En nuestro caso, por ejemplo, *impreb1.ctt.local* (Fig. 8).

Cuando se crea un puerto de red, el sistema comprueba que en esa dirección hay un escuchador capaz de soportar el otro extremo de la comunicación. Para ello, la impresora de red debe estar configurada con su dirección final. Esto se suele hacer mediante el servidor web que incorpora. El fabricante proporciona de fábrica una dirección IP que especifica en la documentación. Sin embargo, para la creación de las colas compartidas en el servidor no es necesario que esté físicamente la impresora.

Después acudiremos a la sección de Impresoras y agregaremos una nueva. El asistente nos pedirá un puerto y nosotros le asignaremos el puerto de red (TCP/IP) que hemos creado anteriormente para ella. Posteriormente nos pedirá que le asociemos un controlador. Como es la primera impresora que creamos, decidimos instalar un nuevo driver de impresión.

Este es el momento de indicar el modelo de la impresora (en la figura, Lexmark E120n) para que el sistema elija el controlador adecuado. Después el asistente nos pedirá un nombre lógico para la impresora y, si queremos compartirlo en la red como es nuestro caso, el nombre con el que se compartirá (en nuestro caso el mismo nombre de la impresora), y algunos detalles sobre su ubicación (Fig. 9).

Procederemos de modo semejante con la impresora *ImpreA1*, que también es una impresora de red. Una vez creadas las impresoras tendremos que asignar permisos para cada una de ellas. En concreto queremos que por *ImpreB1* pueda imprimir solo el bibliotecario, por *ImpreA1* solo los investigadores y el bibliotecario (Fig. 10,

derecha), mientras que por *ImpreB2* (que será local al servidor) podrán imprimir todos los usuarios.

En el caso de la impresora local al servidor *ImpreB2* todo será igual excepto que el puerto elegido no será un puerto de red sino que será un puerto local, en nuestro caso el puerto LPT1 que es un puerto paralelo (Fig. 10, izquierda).

Después de estas operaciones, las impresoras serán servidas a la red a través de las colas de impresión de SRV y los clientes podrán conectarse remotamente a ellas a través de este servidor (Fig. 11).

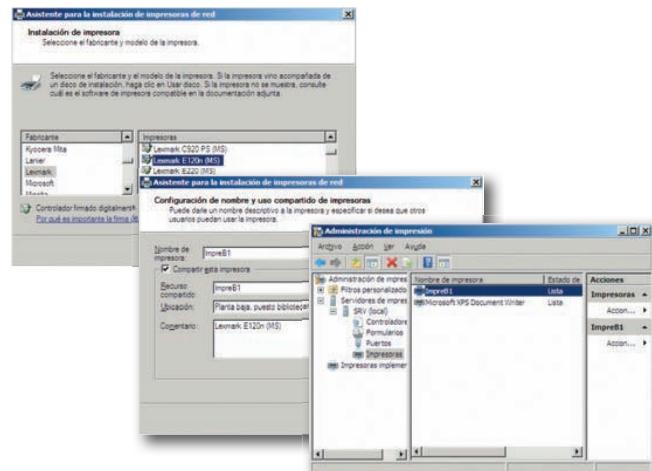


Fig. 9. Elección del controlador de la impresora, compartición en red y vista de la consola de administración con la nueva impresora creada y compartida.

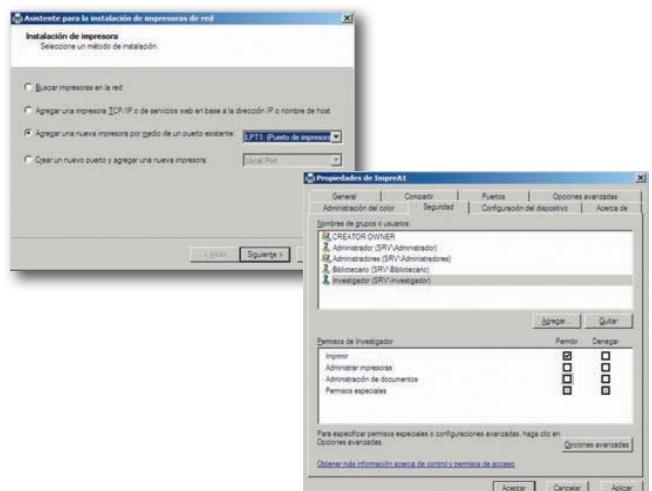


Fig. 10. Elección de un puerto local (LPT1) para una impresora local servida en la red (a la izquierda) y asignación de permisos de impresión para una impresora (a la derecha).

Práctica final

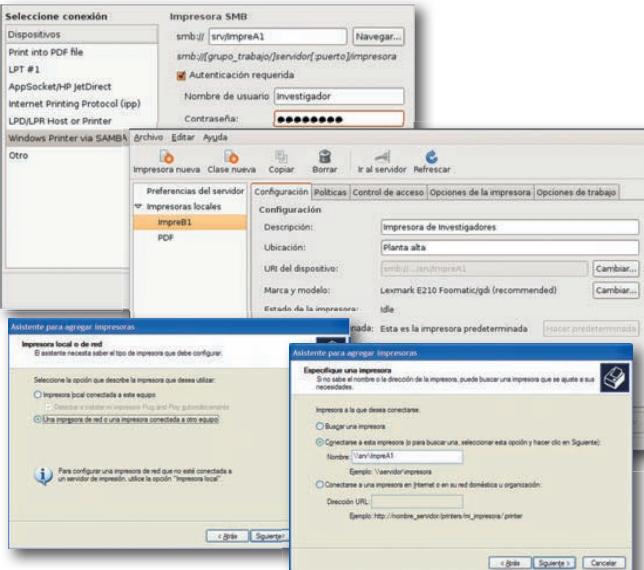


Fig. 11. Secuencia de conexión a una cola de impresora remota desde una estación cliente Linux (arriba) y Windows (abajo).

6. Carpetas compartidas

El servicio de carpetas compartidas lo realizaremos a través de CIFS/SMB, el protocolo de Microsoft para compartir carpetas e impresoras equivalente al Samba utilizado en equipos Linux, de modo que podremos utilizar el sistema de nombres NetBIOS y seremos compatibles tanto con clientes Windows como con clientes Linux, ya que NetBIOS puede correr sobre TCP/IP.

Hay que crear las carpetas que queramos compartir, a las que habrá que asignarles los permisos para que solo los usuarios autorizados puedan utilizarlas:

- C:\FondosBiblioteca: con información para cualquier usuario.
- C:\FondosInvestigadores: con información accesible solo a investigadores.

El bibliotecario podrá acceder a todos los recursos.

Seleccionamos la carpeta en el explorador de archivos y con el botón derecho indicamos «Compartir esta carpeta». Un asistente nos preguntará el nombre de compartición y los derechos de acceso (Fig. 12).

CEO

SMR_RL_AAbad_09_Bloque2_Impresoras.pptx

Documento que contiene información sobre instalación y configuración de las colas de impresoras compartidas.

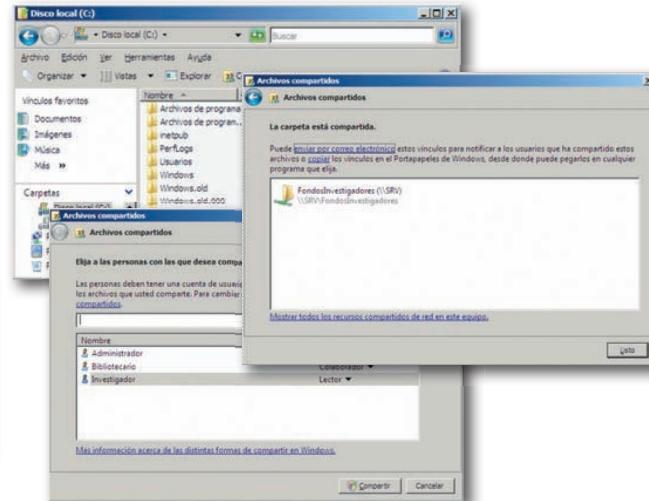


Fig. 12. Pasos para compartir una carpeta a la red.

CEO

SMR_RL_AAbad_09_Bloque2_Impresoras.pptx

Documento que contiene información sobre instalación y configuración de las colas de impresoras compartidas.

Ahora desde las distintas estaciones clientes podemos probar si hemos compartido bien las carpetas realizando unas pruebas de conexión mediante los asistentes de conexión a carpetas compartidas (Fig. 13).

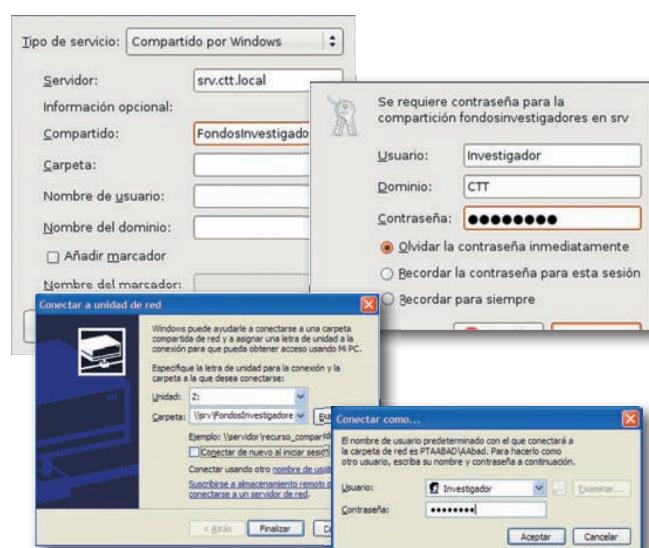


Fig. 13. Secuencia de conexión a una carpeta de red desde un cliente Linux (arriba) y Windows (abajo).