Unidades de competencia
Certificados de profesionalidad

Ciclo Formativo Grado Medio

Redes locales

Alfredo Abad Domingo

Mc Graw Hill Education

www.mhe.es/cf/informatica

Redes locales

Alfredo Abad Domingo

Mc Graw Hill Education

MADRID - BARCELONA - BOGOTÁ - BUENOS AIRES - CARACAS - GUATEMALA
MÉXICO - NUEVA YORK - PANAMÁ - SAN JUAN - SANTIAGO - SÃO PAULO
AUCKLAND - HAMBURGO - LONDRES - MILÁN - MONTREAL - NUEVA DELHI - PARÍS
SAN FRANCISCO - SIDNEY - SINGAPUR - ST. LOUIS - TOKIO - TORONTO

Redes locales · Ciclo Formativo de Grado Medio

McGraw-Hill/Interamericana de España, S.L.
Edificio Valrealty, 1.ª planta
Basauri, 17
28023 Aravaca (Madrid)

ISBN: 978-84-481-8552-7

Obra original: *Redes locales* © 2012,
respecto a la segunda edición en español, por McGraw-Hill Interamericana de España, S.L.

ISBN edición original: 978-84-481-8082-9

© Alfredo Abad Domingo
Autor del material complementario: Alfredo Abad Domingo
Equipo editorial: Ariadna Allés, Paloma Sánchez, Silvia García Olaya
Diseño de cubierta: RLoad.es
Diseño interior: Reprotel, S.L.
Fotografías: 123RF, Getty
Ilustraciones: Pablo Blasberg
Composición: Artesa, S.L.

Presentación

Uno de los campos con mayor relevancia en la sociedad actual está abanderado por las Nuevas Tecnologías, especialmente una serie de técnicas que se han agrupado bajo el nombre de Tecnologías de la Información y de la Comunicación (TIC) o, más recientemente, Tecnologías de la Información, abreviado IT en inglés.

Las TIC proporcionan una amalgama entre la informática, las redes de comunicación y la multimedia, existiendo entre ellas una estrecha colaboración y beneficiándose cada una de los progresos de las otras. Esta obra pretende fijarse en los aspectos técnicos y procedimentales de las redes locales.

Se ha querido recoger en lengua inglesa la terminología de los términos técnicos, aunque también se proporciona la traducción a la lengua española. La razón que invita a escribir de esta manera reside en la dificultad que entraña leer libros y manuales técnicos sin conocer la terminología inglesa de los conceptos implicados.

El texto se ha estructurado en cuatro bloques temáticos en los que se desarrollan contenidos complementados por otro bloque práctico que se resuelve paulatinamente al final de cada uno de estos bloques temáticos, componiendo de este modo una unidad práctica final (Unidad 9) que se hace transversal a todo el texto.

Cada unidad de contenido finaliza con un conjunto de ejercicios propuestos para estudio y evaluación estructurados por objetivos y orden de dificultad. Además, en la mayor parte de los epígrafes se proponen temas de investigación o de ampliación de conocimientos. Muchos de estos elementos hacen referencia a información residente en la web, de modo que el lector se acostumbre a utilizar Internet como una herramienta más de su trabajo. Las ampliaciones de contenido no son necesarias para cubrir el programa de contenidos y procedimientos sugeridos por la Ley Educativa para el módulo de Redes Locales del Ciclo Formativo de Grado Medio de Sistemas Microinformáticos y Redes, sin embargo, sugieren elementos educativos de ampliación que permiten el acceso a tecnologías novedosas o inducen a conseguir un conocimiento más profundo del contenido teórico.

Es importante utilizar algunas de estas ampliaciones y sugerencias de investigación para desarrollar en el lector el suficiente espíritu crítico e investigador que le permita posteriormente reciclarse en su profesión en el transcurso de su vida profesional.

También se proponen a lo largo del texto algunos ejercicios y actividades para realizar en grupo con el objetivo de acostumbrar a los alumnos a trabajar en equipo y a comprender que un proyecto puede resolverse con diversas propuestas, estimulando de este modo valores como la tolerancia, saber escuchar a los demás, el respeto por las opiniones ajenas, el trabajo cooperativo, etc.

Los casos prácticos que aparecen resueltos a lo largo del texto están contextualizados en el entorno profesional. Así, el lector concebirá los conceptos que se explican y repetirá los procedimientos que se sugieren motivado por una actividad profesional concreta. Se ha considerado como algo muy importante en el desarrollo del texto que el lector conozca de antemano para qué sirve aquello que estudia.

En esta segunda edición del texto se han incorporado las novedades tecnológicas que se han ido consolidando desde la edición anterior, se ha añadido un mapa conceptual a modo de síntesis por cada unidad y se ha incorporado un nuevo test de repaso resuelto que sirva al alumno de evaluación continua.

Se recomienda estudiar los contenidos en el orden secuencial en que aparecen. Las primeras experiencias prácticas deben realizarse al final del primer bloque (después de las dos primeras unidades). Aunque en el texto se advierte expresamente, insistimos aquí en que antes de empezar con el primer bloque práctico debe estudiarse en profundidad el primer epígrafe de la unidad práctica final (Unidad 9), en el que se describe detalladamente el enunciado práctico que se resolverá transversalmente a lo largo del curso.

Dedico esta obra a mis padres, de quienes todo lo he recibido.

El autor

Índice

Índice

Cómo se utiliza este libro

Presentación de la unidad

Aquí encontrarás los **criterios de evaluación** de la unidad.

Además te avanzamos los **contenidos** que se van a desarrollar.

Desarrollo de los contenidos

Caso práctico

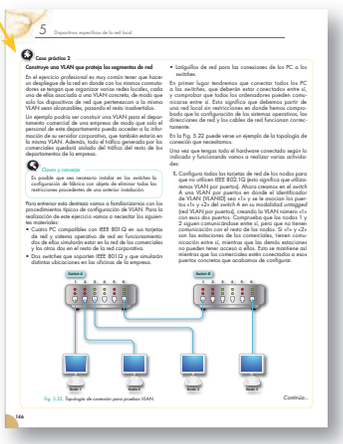
Aplican los conocimientos aprendidos a problemas y situaciones reales del entorno profesional.

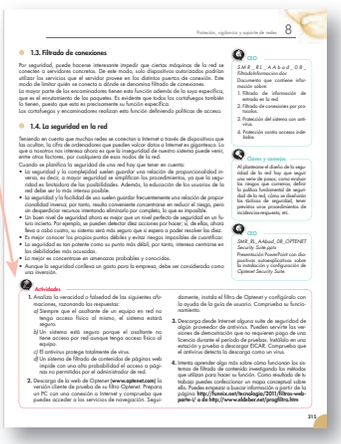
Actividades

Permiten trabajar los contenidos a medida que se van explicando y aseguran un aprendizaje progresivo.

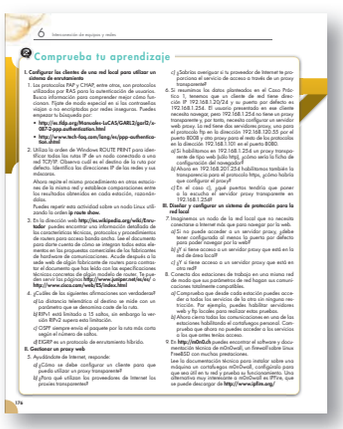
Una exposición clara y concisa de la teoría, acompañada de recuadros que ayudan a la comprensión de los aspectos más importantes:

- **Ampliación**
- **Seguridad**
- **Truco**
- **Investigación**
- **Claves y consejos**
- **Vocabulario**





Cierre de la unidad



SÍNTESIS
Esquema resumen de los contenidos estudiados en la unidad.

TEST DE REPASO
Ayuda a detectar cualquier laguna de conocimientos.

COMPRUEBA TU APRENDIZAJE
Actividades finales agrupadas por criterios de evaluación.

PRÁCTICA FINAL
Ejercita de forma integrada las competencias adquiridas.

Unidad 1

Caracterización de redes locales

En esta unidad aprenderemos a:

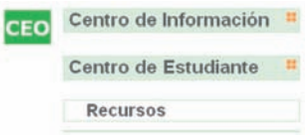
- Conocer las fuentes de información de estándares.
- Identificar los distintos tipos de redes.
- Identificar los elementos de una red.
- Reconocer las distintas topologías de red.
- Conocer la composición de la arquitectura de red estándar OSI.

Y estudiaremos:

- Las familias de protocolos.
- Las topologías de red.
- El modelo de referencia OSI para redes.
- Los dispositivos que se pueden conectar a las redes.

CEO

En el **Centro de Enseñanza Online** de este libro **http://www.mhe.es/cf/informatica** encontrarás todos los documentos mencionados en los cuadros CEO.



Vocabulario

Teleinformática o **Telemática:** es la técnica que trata de la comunicación remota entre procesos. Para ello, debe ocuparse tanto de la interconectabilidad física —forma del conector, tipo de señal, parámetros eléctricos, etc.—, como de las especificaciones lógicas: protocolos de comunicación, detección y corrección de errores, etc.

Red entre iguales, *peer-to-peer* o p2p: es una red en la que todos los nodos se comportan como clientes y servidores simultáneamente de modo que cualquier servicio es brindado a la red directamente al cliente que lo solicita sin necesidad de intermediarios.

Tasa de error: en una transmisión es la proporción entre los bits erróneos y los bits totales transmitidos. En la jerga profesional, cuando la tasa de error de una transmisión se dispara, se dice que la «línea tiene ruido».

Investigación

Utiliza la información que puedes encontrar en Wikipedia **(es.wikipedia.org)** por la voz *peer to peer* para descubrir los distintos tipos de redes punto a punto que hay, así como sus diversos campos de aplicación.

1. Introducción

Las redes de área local se organizan como un conjunto de protocolos de comunicación que operan sobre una topología bien definida que les indican cómo se conectan los ordenadores de la red.

En esta unidad estudiaremos algunos modelos básicos de redes de área local así como algunas de sus implementaciones, especialmente de las redes TCP/IP como núcleo tecnológico de Internet y del modelo de referencia internacional estándar OSI.

Los ordenadores son máquinas especializadas en procesar información de acuerdo con las instrucciones recogidas en un programa. Sin embargo, no siempre la información se produce o se almacena en el lugar donde se procesa. Esto añade la necesidad de transportar los datos desde su lugar de origen o almacenamiento hasta el de su proceso, originando una comunicación.

La base de cualquier comunicación es una transmisión de señal. Las redes de ordenadores vienen a cubrir estos dos aspectos: transmisión y comunicación.

A través del cableado de la red se pueden transmitir señales eléctricas adecuadas a la naturaleza del cable, pero la red no solo debe entregar esta señal en su destino, sino que además debe garantizar que la información que originó el emisor llega al receptor, de modo que el mensaje permanezca íntegro durante el recorrido.

2. Redes de área local

Una red de área local (LAN, *Local Area Network*) es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un área privada y restringida. La red de área local tiene, entre otras, las siguientes características:

- Una restricción geográfica: el ámbito de una oficina, de la planta de un edificio, un edificio entero, e incluso, un campus universitario: depende de la tecnología con que esté construida.
- La velocidad de transmisión debe ser relativamente elevada.
- La red de área local debe ser privada, toda la red pertenece a la misma organización.
- Fiabilidad en las transmisiones. La **tasa de error** en una red de área local debe ser muy baja.

Desde el punto de vista operativo, la principal función de una red consiste en que los ordenadores de la red puedan compartir recursos mediante el intercambio de paquetes de datos entre los distintos equipos conectados a la línea de transmisión.

Hay dos maneras fundamentales de conexión de ordenadores personales en una red dependiendo de la ubicación de los recursos. La forma básica consiste en hacer que todos los ordenadores pongan a disposición de los demás los recursos de que disponen, fundamentalmente discos e impresoras. Bajo esta concepción de red, ningún ordenador está privilegiado, todos tienen las mismas funciones.

Tecnológicamente, este modo de organización es muy simple, pero se hace muy difícil el control de los recursos, puesto que los accesos cruzados son posibles en cualquier dirección. A este tipo de redes se les llama **redes entre iguales.**

Fig. 1.1. *Tres vistas de un armario de servidores. En el centro, vista lateral con las puertas del armario desmontadas para facilitar la instalación. A la izquierda y a la derecha, dos vistas frontales.*

Un segundo modo de organizar la red consiste en privilegiar al menos a uno de los ordenadores añadiéndoles capacidades en forma de servicios, por ello a estos ordenadores se les llama servidores o *servers*. El resto de los ordenadores de la red solicitarán servicios a estos servidores que estarán altamente especializados en la función para la que fueron diseñados, creando así una estructura centralizada en la red.

Este tipo de organización es mucho más fácil de controlar puesto que la administración de los servicios de la red está centralizada, lo que permite automatizar en mayor grado el trabajo del administrador. Los servidores de red llevan incorporado un sistema de cuentas y contraseñas de entrada que restringe los accesos a usuarios no autorizados. A este tipo de organización de la red se le llama **cliente-servidor.**

3. Redes de área extensa

Una red de área extensa o extendida (WAN, *Wide Area Network*) es una red que intercomunica equipos en un área geográfica muy amplia.

Las transmisiones en una WAN se realizan a través de líneas públicas. La capacidad de transmisión de estas líneas suele ser menor que las utilizadas en las redes de área local. Además son compartidas por muchos usuarios a la vez, lo que exige un acuerdo en los modos de transmisión y en las normas de interconexión a la red.

Las tasas de error en las transmisiones en las redes de área extensa son mayores —unas mil veces superior— que su equivalente en las redes de área local.

Las posibilidades de las redes de área extendida son enormes: distintos tipos de redes de área local que interconectan, equipamientos de diversos fabricantes, multitud de protocolos de comunicación, posibilidad de diferentes líneas de transmisión, etc. Las tecnologías también son muchas: Red Digital de Servicios Integrados (RDSI o ISDN), *Frame Relay*, ATM, X.25 o las redes de satélites.

Internet es un ejemplo de red de servicios estructurada sobre una red de área extensa de alcance mundial que utiliza todas las tecnologías a que aludíamos en el párrafo anterior.

Actividades

1. Utiliza la red de área local del aula para habituarte a trabajar en su entorno. Consigue una cuenta de usuario en alguna de las estaciones de la red e inicia una sesión. Describe los nodos y servicios que puedes ver a través de la red. Crea un mapa lógico de estos servicios (discos, impresoras, páginas web útiles) y prueba la funcionalidad de cada uno de ellos.
2. Instala en un ordenador una aplicación p2p para practicar la descarga de algunos ficheros.
3. Una instalación de red quiere añadir dos impresoras a la red. Cada impresora se conecta a través de su interfaz de red. Sobre la primera impresora se desea que puedan imprimir todos los usuarios de la red, pero sobre la segunda impresora se quieren mantener unas ciertas restricciones. ¿Qué modelo de red —cliente/servidor o *peer to peer*— sería el más apropiado para cada una de las impresoras? Razona la respuesta.

Seguridad

La tecnología *peer to peer*, aunque extraordinariamente flexible, entraña unos riesgos importantes: supone una fuente frecuente de transmisión de virus y malware, puede llegar a consumir gran parte del ancho de banda de que dispongamos y puede generar problemas legales por violación de la propiedad intelectual.
En la dirección **http://video.google.com/videoplay?docid=-7012884909062999701&q=sgae** puedes visualizar la videograbación de una conferencia sobre la tecnología p2p.

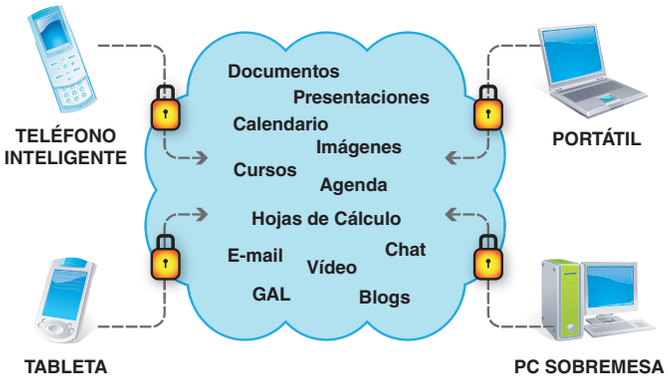


Fig. 1.2. *La computación en la nube proporciona acceso seguro a las aplicaciones desde cualquier dispositivo.*

3.1. Computación en la nube

La computación en la nube *(cloud computing)* es un nuevo modelo de utilización de los recursos informáticos de modo que todo se brinda como servicio deslocalizado. Por ejemplo, aunque se esté trabajando desde un ordenador personal, el espacio de almacenamiento en donde se guardan los ficheros puede estar en un proveedor de almacenamiento al otro lado de Internet (en la nube). Si en un momento dado cambiamos de PC, los datos seguirán estando disponibles en la nube puesto que no residen en el PC local.

Un ejemplo parecido lo tendríamos si ponemos en la nube no solo el almacenamiento, sino también las propias aplicaciones y las bases de datos. El objetivo funcional de la nube es que los usuarios puedan utilizar los recursos desde cualquier dispositivo electrónico (PC, portátil, Smartphone, etc.) situado en cualquier lugar, utilizando como herramienta un navegador de Internet o una aplicación local similar y como medio de acceso Internet.

Además, los servicios consumidos se facturan por uso, lo cual disminuye sensiblemente las inversiones iniciales en tecnología que tienen que hacer las corporaciones cuando comienzan sus despliegues de sistemas y aplicaciones.

Las nubes pueden ser **privadas,** en donde toda la infraestructura necesaria es propiedad del propietario; **públicas,** en donde la infraestructura se contrata con proveedores externos a la corporación que proporcionan servicios públicos; o **híbridas,** en las que se dispone de infraestructuras privadas complementadas con otras públicas.

CEO

SMR_RL_AAbad_01_eyeOS.pptx

Documento que contiene información sobre la secuencia de pasos para probar eyeOS desde su sede web sin necesidad de instalación.

Laboratorio

Utilización de un escritorio virtual web en la nube mediante EyeOS

EyeOS es un sistema operativo en la nube que permite a los usuarios utilizar un escritorio digital en la nube (aplicaciones y datos) a través del explorador de Internet.

Con este sistema se consiguen, entre otras, las siguientes ventajas:

a) **Ubicuidad:** se puede acceder a los propios documentos desde cualquier lugar y desde cualquier dispositivo capaz de ejecutar un navegador de Internet.

b) **Capacidad de colaboración:** varios usuarios pueden compartir sus archivos en la nube.

c) **Seguridad:** cada usuario del sistema puede proteger su información con un sistema de permisos.

d) **Bajo coste:** como en otras aplicaciones en la nube, los costes de despliegue se reducen significativamente.

Algunas de las aplicaciones que permite utilizar el escritorio de EyeOS son:

1. **Ofimáticas:** eyeDocs, eyeSheets, eyePresentation, eyeCalendar, eyeContacts, eyePdf, eyeNotes.
2. **Educativas:** eyePlot, eyeCalc.
3. **Red:** eyeFeeds, eyeNav, eyeMail, eyeBoard, eyeUpload, eyeFTP, eyeMessages.
4. **Multimedia:** eyeMp3, eyeVideo.

EyeOS se puede descargar desde la web **www.eyeos.org** e instalarlo localmente; sin embargo, para utilizarlo no hace falta hacer una instalación. Desde la misma web se puede utilizar una versión de prueba.

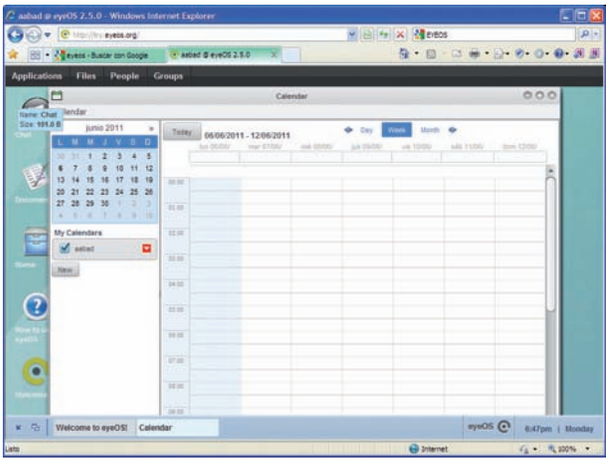


Fig. 1.3. *Escritorio virtual.*

La operación en este ejercicio de laboratorio consistirá en conectarte a Internet, acudir a la web de eyeOS, buscar la página de pruebas y probar el sistema en la nube.

Para ello, una vez que accedas a la página web que te da acceso al escritorio virtual, el sistema te pedirá un nombre de usuario y contraseña.

Crea una nueva cuenta mediante el registro y utilízala para probar el sistema.

Finalmente puedes escribir un documento que describa tu experiencia de usuario respecto a este sistema en la nube.

4. Otras redes

Nos dedicaremos en los siguientes epígrafes a explicar brevemente las características de otras redes: las redes metropolitanas (MAN), redes de área personal (PAN) y las redes de área local inalámbricas (WLAN).

4.1. Redes metropolitanas

Una red metropolitana es una red de distribución de datos para un área geográfica en el entorno de una ciudad. Este tipo de redes es apropiado, por ejemplo, para la distribución de televisión por cable en el ámbito de la población sobre la que se extiende geográficamente la red. Las compañías operadoras de cable compiten activamente con las de telefonía, proporcionando a través del cable toda una oferta de servicios entre los que se encuentran TV, vídeo, Internet y la telefonía tradicional.

4.2. Redes de área personal

Actualmente los ordenadores ya no solo están en los escritorios sino también en las PDA, Tablets, lectores de e-Books, teléfonos móviles, etc. Sin embargo, todos estos dispositivos pierden funcionalidad si permanecen aislados. Esta necesidad de conexión ha llevado a desarrollar una tecnología de redes que recibe el nombre genérico de Redes de Área Personal (PAN, *Personal Area Network*).

Las redes PAN tienen algunas características que las hacen peculiares. Mencionamos aquí algunas de ellas:

- La configuración de acceso a la red debe ser muy sencilla o incluso automática.
- El radio de acción de la red debe ser geográficamente muy limitado, con objeto de que dos redes no colisionen fácilmente entre sí.
- El medio de transmisión por excelencia, aunque no de modo exclusivo, es el inalámbrico.
- Los costes de la red, tanto de instalación como de explotación, deben ser pequeños y en algunas ocasiones sin coste, como en el caso de la conexión de ratones inalámbricos, impresoras por infrarrojos, Bluetooth o Wi-Fi, etc. Por ejemplo, la instalación doméstica de una red Wi-Fi es muy barata, pero el servicio de conexión a Internet que se proporciona a través de esa red inalámbrica tiene el coste exigido por el proveedor de Internet.

4.3. Redes inalámbricas

La comodidad de una instalación sin cables junto con el descenso significativo de los costes de fabricación ha redundado en un importante auge de las comunicaciones telemáticas inalámbricas. Más adelante desarrollaremos exhaustivamente estas tecnologías, pero de momento mencionaremos Bluetooth e Infrarrojos para bajas tasas de transferencia, Wi-Fi para redes de área local y WiMAX para redes metropolitanas. Todas estas tecnologías se agrupan bajo el nombre WLAN *(Wireless Local Area Network)*.

Una WLAN tiene muchas ventajas pero también inconvenientes:

- Al ser aéreo el medio de transmisión y, por tanto abierto a cualquier dispositivo que se encuentre en las cercanías, las redes inalámbricas exponen una mayor superficie de ataque, lo que brinda más posibilidades a los **crackers.**
- Como el canal de transmisión es compartido por todas las estaciones, los sistemas inalámbricos tienen que multiplexar las señales de transmisión repartiendo el ancho de banda del canal entre todas las estaciones inalámbricas, lo que frecuentemente produce situaciones de congestión.

La seguridad es siempre importante en toda comunicación, pero cobra un especial relieve en las redes inalámbricas. Esto, a veces, complica las instalaciones, reduciendo la gran ventaja que tienen de no tener que instalar cables para conectar en red los equipos.

Actividades

4. Utiliza los teléfonos móviles, portátiles y *palms* o *pocket-pc* que dispongan de tecnologías de infrarrojos o Bluetooth para ensayar conexiones punto a punto o multipunto entre ellos, transferir mensajes y ficheros o utilizar de sus servicios remotos.

Tendrás que ayudarte de los manuales de usuario de estos dispositivos o de su ayuda en línea.

Ten en cuenta que la tecnología de infrarrojos es altamente direccional, es decir, los dispositivos no solo tienen que estar cerca sino que además deben poder verse en línea recta enfrentando sus ventanas de emisión/recepción.

Haz una prueba de cobertura en cada una de las tecnologías. Para ello, intenta hacer una conexión colocando los dos dispositivos uno al lado del otro.

Repite el procedimiento varias veces alejando los dispositivos progresivamente. El límite de cobertura será el punto en donde ya no puedas realizar la conexión. Compara ahora la cobertura de cada una de las tecnologías inalámbricas.

5. ¿Cuántos tipos de nubes hay en relación con el propietario de los servicios?

6. ¿Dónde residen los datos cuando se utiliza cloud computing? ¿Y las aplicaciones?

CEO

SMR_RL_AAbad_01_EstandaresAsociaciones.docx
Documento que contiene información sobre:
1. Estándares de red.
2. Asociaciones de estándares.

Vocabulario

Host o nodo: es un ordenador con capacidad de interactuar en red o capaz de alojar algún tipo de servicio de red.
Estándar: es un conjunto de reglas que regulan algún aspecto de una comunicación para que los productos de distintos fabricantes logren la interoperabilidad entre ellos. Los estándares se recogen en documentos que se hacen oficiales cuando una asociación de estándares internacionales los aprueba.
Protocolo: es el conjunto de reglas que dos ordenadores deben seguir, y que por tanto comparten, para que puedan entenderse.

Investigación

Estudia algunas páginas de información sobre protocolos de red para que puedas descubrir sus funciones más importantes y algunos ejemplos de protocolos estándar que se utilizan en las comunicaciones con redes de ordenadores. Puedes empezar tu búsqueda en Wikipedia por la voz «protocolo de red».

Otra página de interés es **http://fmc.axarnet.es/redes/tema_06.htm** y **http://vgg.uma.es/redes**

CEO

SMR_RL_AAbad_01_Organizacion_Red.docx
Documento que contiene información sobre:
1. Modo de organización de una LAN, sistemas.
2. Sistemas distribuidos frente a centralizados.
3. Factores que hacen necesaria la LAN.

5. Características de la LAN

Salvo las redes p2p, cualquier red de área local está muy lejos de parecerse a una conjunción caótica de ordenadores. Toda la estructura de la red está organizada por la posición geográfica de sus **nodos,** los servicios que provee, la custodia segura de la información, etc.

La organización de **estándares** IEEE proporciona una definición oficial del concepto de red de área local del siguiente modo:

> «Una red de área local se distingue de otros tipos de redes de datos en que las comunicaciones están normalmente confinadas a un área geográfica limitada tal como un edificio de oficina, un almacén o un campus; utilizando un canal de comunicación de velocidad moderada o alta y una tasa de error baja».

En esta definición de la IEEE se observan claramente los elementos esenciales de cualquier red de área local: ámbito, seguridad y velocidad.

Otro elemento que caracteriza profundamente a una red es el conjunto de **protocolos** que utiliza para comunicarse.

Denominamos protocolo abierto a aquel que se acoge a los estándares internacionales y que es implementado por muchos fabricantes. Frente a este, tenemos el protocolo cerrado o propietario, que es diseñado por compañías concretas y se exigen licencias de uso a cuantos fabricantes quieran incorporarlos a sus sistemas de comunicación.

Otras características que aparecen frecuentemente en las redes de área local y que están relacionadas entre sí son:

- Los canales de transmisión suelen ser de tipo multiacceso. Los nodos utilizan un único canal para comunicarse con el resto de los equipos que componen la red. Todos los paquetes de red, que los nodos escriben en el canal, son enviados indistintamente a todos los nodos de la red o bien a subconjuntos concretos de estos equipos.
- Las líneas de comunicación suelen ser multipunto, a diferencia de las redes WAN en donde la conexión suele ser punto a punto a través de centrales de conmutación o equipamientos de funcionalidad semejante.
- El tipo de red depende del tipo de cableado. Un cableado apropiado para el acceso a una red WAN, como el cable de pares telefónico, no tiene la calidad requerida para cumplir las especificaciones de velocidad en una red de área local.
- El tipo de red también depende de la topología y de los protocolos utilizados. Las redes de área local admiten cualquier topología, mientras que las redes WAN suelen ser mallas de nodos y centrales conmutadoras. Difícilmente una red en anillo puede constituir el núcleo de una gran red de área extensa, los anillos más grandes no pueden superar los 200 km de perímetro.

Actividades

7. Sobre una instalación de red real identifica los ordenadores que tienen la función de servidores y aquellos otros que hacen de clientes. Localiza las zonas de la instalación que son cliente-servidor, las distribuidas y, si las hubiera, las islas de información. Puedes realizar esta identificación sobre la red del aula o laboratorio o programar una visita a las instalaciones de una empresa que tenga un despliegue informático en red.

8. Una interconexión de ordenadores en que cada uno se puede comunicar con cualquier otro sin intermediarios, ¿es propio de una red de área local o de una red de área extensa?

9. Enumera en una doble lista un conjunto de protocolos de red y otro conjunto de servicios de red. ¿Te ayudan estas listas a comprender las diferencias entre servicio y protocolo?

6. Topologías de red

La topología de una red es la propiedad que indica la forma física de la red, es decir, el modo en que se disponen los equipos y el sistema de cableado que los interconecta para cumplir su función. Aunque es posible especificar tres topologías básicas, que describiremos a continuación, en las instalaciones reales se suelen mezclar varias topologías.

6.1. Topología en estrella

En las redes que tienen su topología en estrella, las estaciones se conectan entre sí a través de un nodo especialmente privilegiado que ocupa la posición central de la red, y que forma con el resto de las estaciones una estrella (Fig. 1.4). A este nodo se le denomina estación concentradora de la estrella.

Puesto que a cada nodo le llega un único cable de red, las conexiones suelen ser más estructuradas que en el caso del cableado en bus. Sin embargo, el problema de la topología en estrella se presenta en el entorno del concentrador ya que todos los segmentos deben terminar en él, lo que produce una importante madeja de cables.

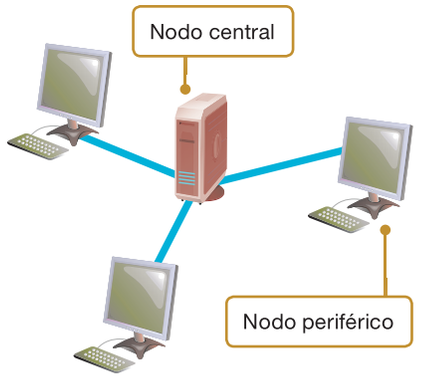


Fig. 1.4. *Esquema de topología de red en estrella.*

6.2. Topología en anillo

Una red en anillo conecta todos sus equipos en torno a un anillo físico (Fig. 1.5). Tampoco presenta problemas de congestión de tráfico; sin embargo, una rotura del anillo produce el fallo general de la red. Un ejemplo concreto de red en anillo es la red «Token Ring», que sigue el estándar IEEE 802.5. Las redes en anillo utilizan protocolos libres de colisiones con técnicas de paso por testigo.

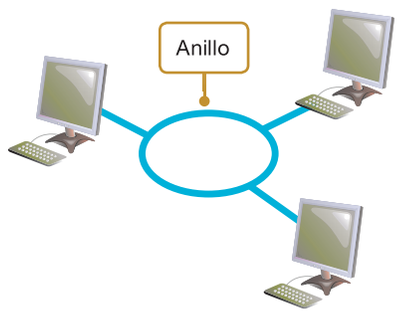


Fig. 1.5. *Topología de red en anillo.*

6.3. Topología en bus

Los puestos de una red en bus se conectan a una única línea de transmisión (bus) que recorre la ubicación física de todos los ordenadores (Fig. 1.6). Esta red es muy simple en su funcionamiento, sin embargo es muy sensible a problemas de tráfico o a las roturas de los cables. Ethernet sobre cable coaxial es un ejemplo de red con topología en bus que sigue el estándar IEEE 802.3.

Las redes de área local con topología en bus son las más sencillas de instalar. No requieren dispositivos complicados para realizar las conexiones físicas entre nodos. Todos los equipos que se conectan a la red lo hacen a través de componentes pasivos o que requieren poca electrónica.

El medio de transmisión que forma la red es un único bus multiacceso compartido por todos los nodos, por lo que se debe establecer una contienda para determinar quién tiene derechos de acceso a los recursos de comunicación en cada instante. Este sistema de contienda determina el tipo de red.

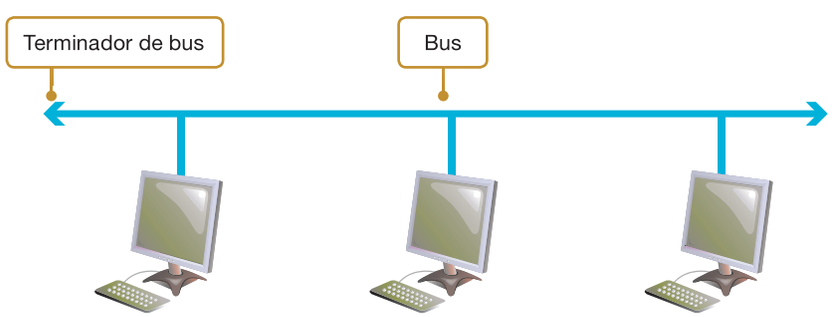


Fig. 1.6. *Topología de red en bus.*

Actividades

10. Seguimos trabajando sobre la instalación de red de área local de ejercicios anteriores. Ahora, identifica los rasgos topológicos de la red. Si es una red grande, ten en cuenta que probablemente la instalación no siga una topología concreta y perfectamente definida, sino que participará de una mezcla de topologías básicas.

11. Comenta qué problemas se pueden generar en una red de cada topología estudiada cuando se rompe uno de los segmentos de red, por ejemplo, la conexión entre dos estaciones contiguas en un anillo, el bus de una red en árbol, etc.

12. ¿Cómo se llaman los estándares de la red Ethernet? ¿Y el de la red Token Ring?

Vocabulario

Protocolo: es un conjunto de reglas perfectamente organizadas y convenidas de mutuo acuerdo entre los participantes en una comunicación, cuya misión es regular algún aspecto de esta.

7. Familias de protocolos

El estudio de las tecnologías de redes se simplifica estructurando las distintas tecnologías involucradas en las comunicaciones en familias de protocolos de comunicación en las que se definen perfectamente las relaciones de unos con otros.

7.1. Conceptos preliminares

Es habitual que los protocolos estén expuestos públicamente como normativas o recomendaciones de las asociaciones de estándares. Los fabricantes que se ajustan a estas normativas tienen la seguridad de ser compatibles entre sí en aquellos aspectos regulados por el **protocolo.**

CEO

SMR_RL_AAbad_01_OtrasTopologiasRed.doc

Documento que contiene información sobre:

1. Topologías de red menos comunes.
2. Topologías mixtas.

A. El concepto de capa o nivel

Con el fin de simplificar la complejidad de cualquier red, los diseñadores de redes han convenido estructurar las diferentes funciones que realizan y los servicios que proveen en una serie de niveles o capas.

Además, en esta estructuración también se consiguen normalizar o estandarizar las técnicas de comunicación favoreciendo la conectividad entre equipos de diversos fabricantes que comparten estándar.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones varían con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

B. La interfaz entre capas

Hemos asentado que dos capas consecutivas establecen relaciones de comunicación. Podemos afirmar que estas relaciones son las únicas que existen en las redes estructuradas como sucesión ordenada de capas. Esto nos lleva a definir el modo en que cada capa negocia los servicios y se comunica con las capas adyacentes. Llamamos interfaz o *interface* de capa a las normas de intercomunicación entre capas.

Ejemplos

Imaginemos un viaje en tren. El viajero debe adquirir un billete, y para ello utiliza un servicio concreto. Pero para llegar a su destino no basta con adquirir el billete. La compañía ferroviaria debe conducirle al tren y situarle en su asiento. A su vez, el tren requiere fluido eléctrico suministrado por la compañía eléctrica para que se pueda producir el fenómeno del transporte. Cada uno de estos acontecimientos pertenece a una capa. Solo pueden solicitarse servicios a las capas adyacentes, por ejemplo, el viajero no puede pedir a la compañía eléctrica el fluido, solo el tren es el que está capacitado para alimentarse eléctricamente de los tendidos de tensión eléctrica.

C. La arquitectura de una red

La arquitectura de red es el conjunto organizado de capas y protocolos que la red utiliza para producir sus comunicaciones entre nodos.

Esta organización de la red debe estar suficientemente clara como para que los fabricantes de software o hardware puedan diseñar sus productos con la garantía de que funcionarán en comunicación con otros equipos que sigan las mismas reglas, es decir, para que sean **interoperables.**

Ejemplos

En el ejemplo del epígrafe anterior existe una forma concreta de solicitar un billete: hay que dirigirse a la ventanilla, esperar un turno, solicitar un destino, etc. Para subirse al tren hay que averiguar el número de andén, desplazarse hasta el mismo, buscar el asiento, etc.

Se dice que dos equipos son **interoperables** cuando siendo de distinta tecnología o de diferentes fabricantes son funcionalmente compatibles entre sí.

Obsérvese que no se han incluido en la arquitectura los interfaces. Ello es debido a que la estructura de capas los oculta totalmente. Una interfaz concreto requiere ser conocido exclusivamente por las dos capas adyacentes a las que separa.

D. Los sistemas abiertos

El concepto de sistema abierto fue propuesto inicialmente por la ISO *(International Organization for Standardization)* como «aquel sistema compuesto por uno o más ordenadores, el software asociado, los periféricos, los procesos físicos, los medios de transmisión de la información, etc., que constituyen un todo autónomo capaz de realizar un tratamiento de la información».

Claves y consejos

En la práctica profesional es muy importante fijarnos en cómo los distintos elementos de la red, proporcionados por los fabricantes, cumplen con los estándares internacionales. En ocasiones se venden dispositivos que implementan una funcionalidad no recogida en un estándar concreto que aún está en fase de aprobación. En este caso, hay que asegurarse de que el dispositivo se podrá actualizar al nuevo estándar una vez que haya sido terminado de definir y aprobado por las organizaciones internacionales de estándares.

Vocabulario

Arquitectura de una red: es el conjunto organizado de capas y protocolos que la red utiliza para producir sus comunicaciones entre nodos.

7.2. Familias de protocolos usuales

OSI define un modelo de referencia para el estudio de las redes del que nos ocuparemos más adelante en profundidad. Sin embargo, las redes comerciales no son totalmente OSI, participan de su modo de estructurar los protocolos, pero cada compañía diseña la red de acuerdo con las tecnologías de las que es propietaria.

Aquí vamos a registrar unas breves referencias de algunas de estas familias más comunes, aunque la más extendida desde el advenimiento de Internet es, sin duda alguna, la familia TCP/IP.

A. Familia NetWare

NetWare, fabricado por Novell, ha sido el sistema operativo de red más utilizado a nivel mundial. Su alto rendimiento, su capacidad de crecimiento (escalabilidad) y, fundamentalmente, la optimización de los recursos requeridos tanto en las estaciones clientes como en las servidoras, han promocionado su utilización masiva.

Los servidores NetWare han sido tradicionalmente dedicados, es decir, no pueden actuar como clientes. El resto de las estaciones son exclusivamente clientes de estos servidores. NetWare utiliza un protocolo propietario desarrollado por Novell, denominado **IPX/SPX** (*Internetwork Packet eXchange/Sequenced Packet eXchange*, Intercambio de paquetes entre redes/Intercambio secuencial de paquetes), derivado de la red de Xerox XNS (*Xerox Network Service*, Servicio de red de Xerox) de Xerox.

Algunos sistemas operativos como Windows, incorporan protocolos clónicos del IPX. En concreto los sistemas de Microsoft lo llaman NWLink (Fig. 1.7).

En la Fig. 1.7. (arriba) se ven instalados los protocolos IPX/SPX propios de la red NetWare (NWLink en Microsoft) y TCP/IP. Obsérvese que ambos protocolos pueden convivir perfectamente sobre la misma interfaz de red (en nuestro caso una tarjeta de red Broadcom NetXtreme).

Abajo configuramos un número de red, que la identifica unívocamente y además elegimos el tipo de trama (nivel 2 de OSI) que escuchará nuestra red.

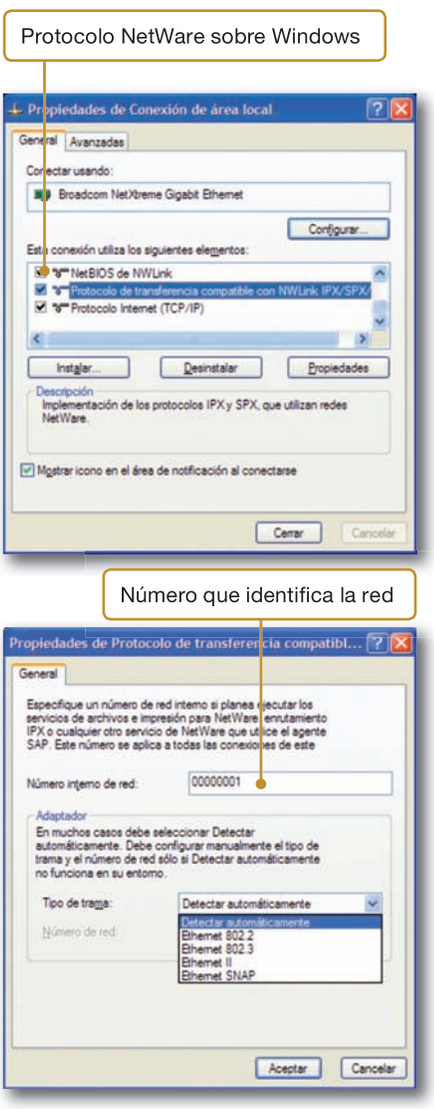


Fig. 1.7. *Instalación y configuración de los protocolos NetWare en una estación Windows XP.*

NWLink no basta para beneficiarse de los servicios proporcionados por un servidor NetWare. IPX o NWLink son protocolos equivalentes de la capa de red en OSI. Para conseguir la utilización de los servicios necesitan crear sesiones basadas en estos servicios, lo que se consigue incorporando un ***REDIRECTOR.*** En estaciones Windows, este redirector se denomina «Servicio cliente de NetWare» (Fig. 1.8), aunque a partir de Windows Vista Microsoft ya no incorpora los protocolos de la red NetWare de modo nativo.

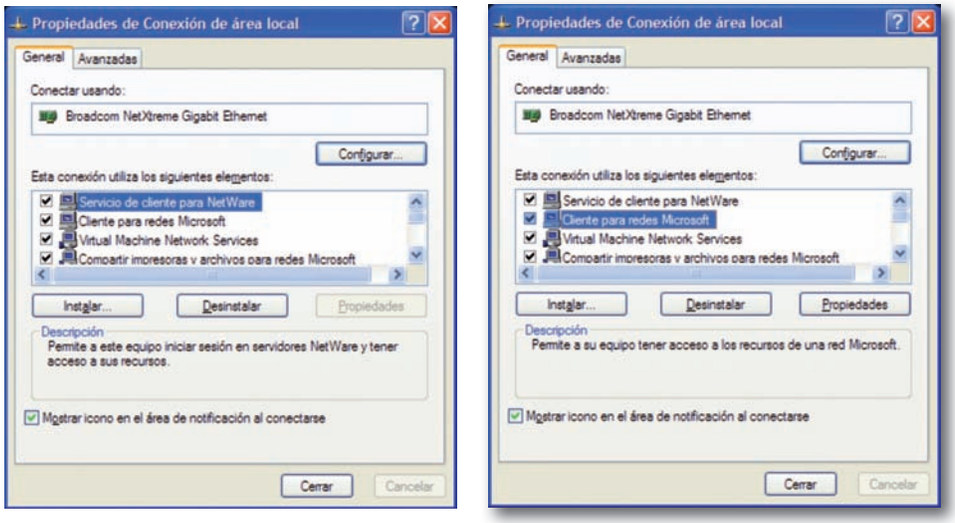


Fig. 1.8. *Instalación y configuración de redirectores de red para redes NetWare (a la izquierda) y para redes Microsoft (a la derecha) en una estación Windows conviviendo sobre la misma interfaz de red.*

B. Familia NetBeui

Microsoft dispone de diversos sistemas operativos para resolver las comunicaciones en las redes de área local, todos ellos pensados para convivir en una red. Los sistemas operativos de Microsoft son una base para la construcción de redes entre iguales utilizando **NetBeui,** que es un protocolo desarrollado por IBM en 1985.

Algunos protocolos se encargan exclusivamente de la manipulación de datos, otros, en cambio, se ocupan del intercambio de mensajes entre las aplicaciones de red. NetBeui es un protocolo que controla tanto los datos como los mensajes entre aplicaciones. Cuando un sistema operativo de red implementa el protocolo NetBeui, los servicios son alcanzados a través de la interfaz **NetBIOS** que actúa como su REDIRECTOR nativo.

Truco

Actualmente, aunque todos los sistemas Windows de Microsoft «hablan» NetBeui, lo más frecuente, además de recomendado, es construir redes de sistemas de Microsoft utilizando TCP/IP, protocolo que también incorporan como nativo.

Como NetBIOS es una interfaz de software que separa dos niveles de red, puede recibir peticiones de las capas superiores de la red y comunicar con los niveles inferiores con independencia de la tecnología de estas capas inferiores. Por ello, si el fabricante del software de la red lo ha programado, podrá utilizarse la interfaz NetBIOS en su red. En el caso de la figura, se ha conectado NetBIOS tanto a la red NetWare (NWLink) como a la red TCP/IP.

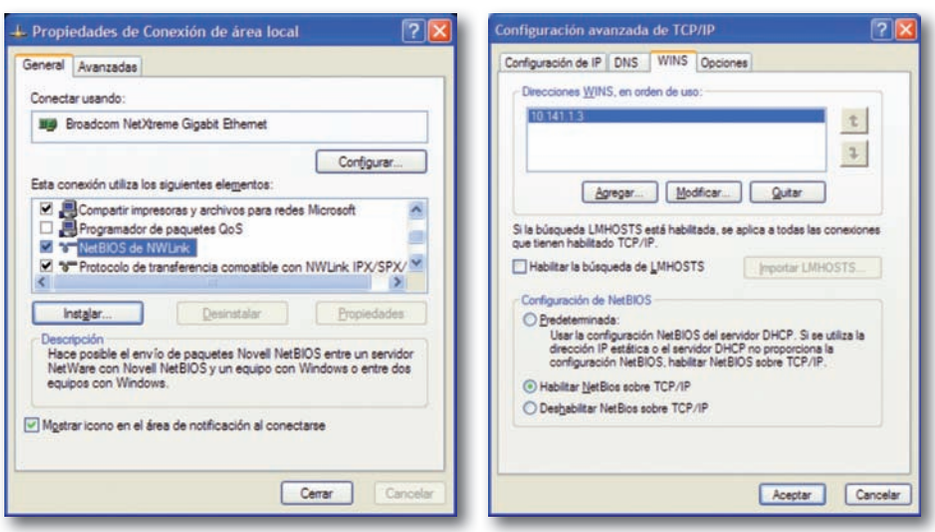


Fig. 1.9. *Instalación y configuración de la interfaz NetBIOS para redes NetWare y TCP/IP en Windows.*

C. Familia AppleTalk

AppleTalk es el nombre de la red entre iguales diseñada por Apple para sus Macintosh. El diseño original se pensó para compartir ficheros e impresoras entre los usuarios de la red de modo que su configuración fuera tan sencilla que incluso un usuario no experto pudiera realizarla.

El primer diseño de AppleTalk fue una sencilla red que resolvía la conexión de un Macintosh a una impresora. Sin embargo, con AppleTalk se pueden confeccionar redes muy amplias y complejas.

Actualmente el sistema operativo de Apple está fundamentado en un núcleo UNIX y, por tanto, sin abandonar totalmente AppleTalk, la red nativa que incorpora es una red TCP/IP, que es la específica de los sistemas UNIX.

D. Familia TCP/IP

El sistema operativo UNIX se ha comunicado en red utilizando un conjunto de protocolos que se ha extendido mundialmente. De hecho, esta familia de protocolos se ha convertido en un estándar *de facto*.

La tecnología TCP/IP (*Transmission Control Protocol/Internet Protocol*, Protocolo de control de la transmisión/Protocolo de Internet), está definida en un conjunto de documentos denominados **RFC** *(Request For Comments)* o Petición de comentarios.

La importancia de TCP/IP es tan grande que la mayor parte de las redes hablan TCP/IP, sin perjuicio de que además puedan incorporar otras familias nativas de protocolos. En este libro la mayor parte de los ejemplos sobre configuración de redes se llevarán a cabo siguiendo la tecnología propuesta por esta familia de protocolos, por ello, le prestaremos mucha más atención.

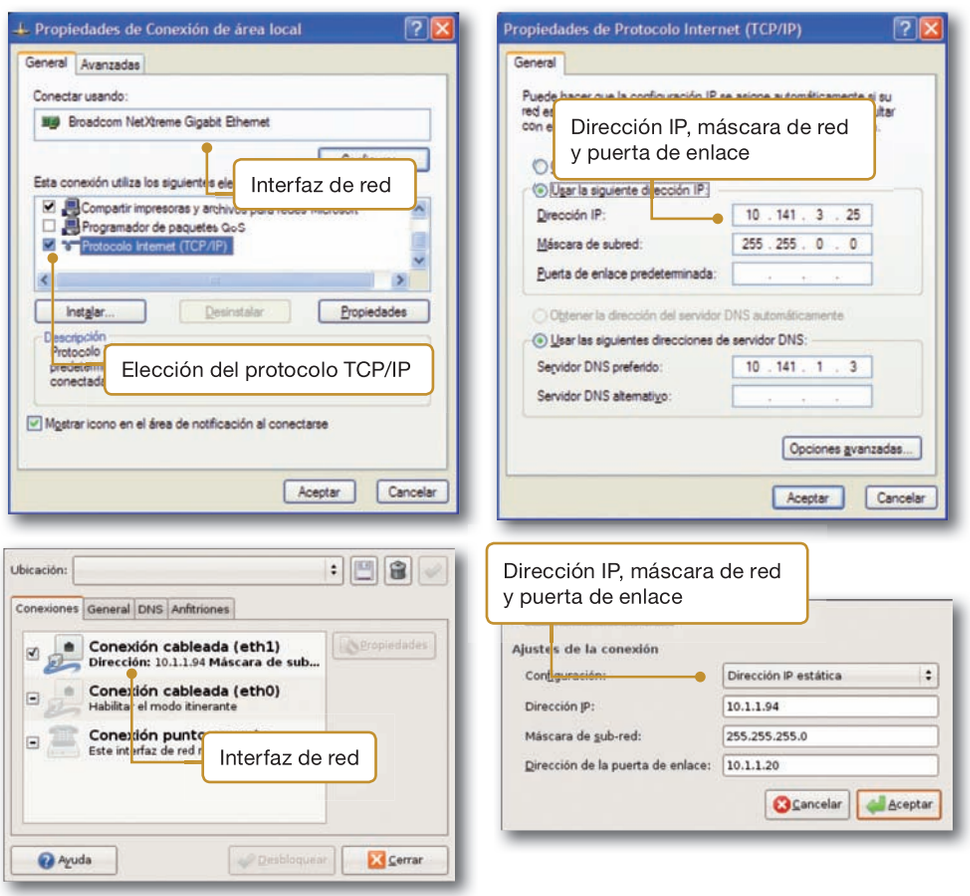


Fig. 1.10. *Instalación y configuración de la red TCP/IP en Windows (arriba) y en Linux (abajo).*

Investigación

Cuando en la práctica profesional se deben adquirir dispositivos de red o decidir sobre los sistemas operativos que se instalarán en los equipos es frecuente tener que tomar las decisiones en función de los protocolos que admiten. Todos estos protocolos están recogidos en los RFC, por eso es conveniente que te familiarices con este tipo de documentos leyendo algunos de ellos. Puedes encontrar información por la voz «request for comments» en Wikipedia. En la web **http://www.faqs.org/rfcs/** puedes encontrar muchos de estos documentos. Por ejemplo, el comentario RFC 821, que puedes leer en la web anterior **(http://www.faqs.org/rfcs/rfc821.html)** y que fue publicado en 1982 explica cómo es el protocolo SMTP utilizado en el envío de correo electrónico.

Actividades

13. Sobre la red de área local objeto de nuestro estudio en estos ejercicios, identifica las familias de protocolos que se utilizan en las comunicaciones entre nodos. Para ello deberás iniciar una sesión en cada ordenador, especialmente en los servidores, para averiguar los protocolos de red instalados a partir de las fichas de características de conexiones de red.

14. ¿Cuál es la familia de protocolos de red más utilizada en la actualidad?

15. ¿Qué es y para qué sirve un RFC?

16. ¿Cuál es el protocolo de red nativo para las redes de ordenadores de Microsoft? ¿Puede convivir este protocolo con otros de otras familias?

8. El modelo de referencia OSI

OSI es el nombre del modelo de referencia de una arquitectura de capas para redes de ordenadores y sistemas distribuidos, propuesta por la ISO como estándar de interconexión de sistemas abiertos.

8.1. Descripción básica de OSI

OSI realmente no es una arquitectura de red sino un modelo de referencia, es decir, un punto de mira desde el que calibrar cómo deben relacionarse unas redes con otras por contraste con un modelo teórico, que es OSI. El modelo propuesto por OSI estructura los servicios de red en siete capas o niveles.

La primera capa es la más cercana al medio físico de transmisión mientras que la séptima capa es la más cercana a las aplicaciones de usuario.

Cuando un usuario necesita transmitir datos a un destino, el sistema de red va añadiendo información de control (cabeceras) para cada uno de los servicios que utilizará la red para ejecutar la orden de transmisión.

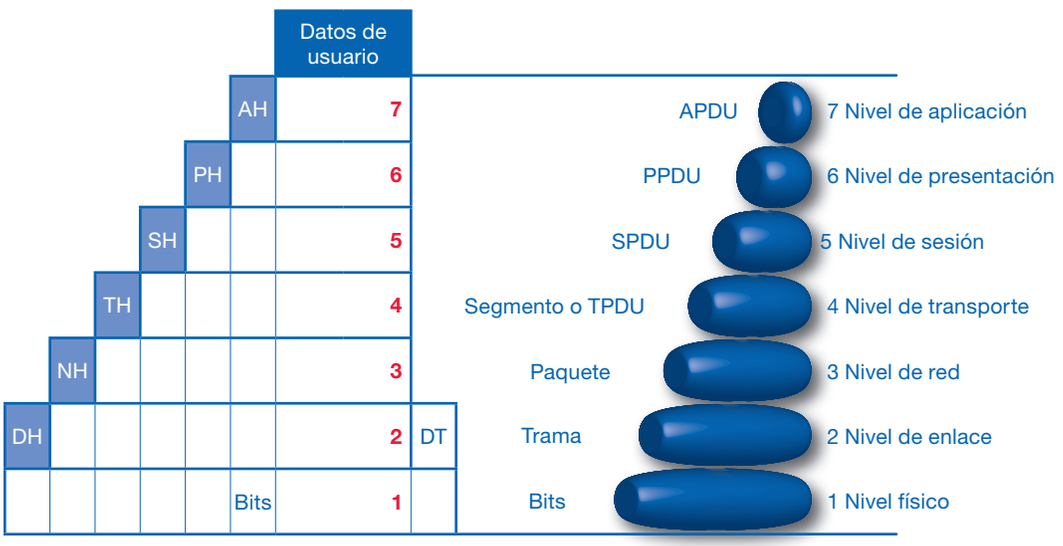


Fig. 1.11. *Cabeceras asociadas a cada nivel OSI (a la izquierda) y su correspondencia en la jerarquía de niveles del modelo OSI (a la derecha).*

Las cabeceras que cada capa añade a los datos que le llegan de su capa inmediatamente superior llevan la información de control necesaria para la interfaz y para la propia capa.

Estas cabeceras, que son específicas en cada nivel, reciben los nombres de AH *(Application header),* PH *(Presentation header),* etc. El nivel 2 incorpora dos campos, uno de inicio DH y otro de final DT, que delimitan la trama.

Ejemplos

Si deseamos enviar un mensaje en papel y es necesario segmentarlo en diversas porciones, cada trozo deberá ir acompañado de una etiqueta identificativa con el fin de poder reconstruir en el destino el mensaje original. La información de numeración de estas etiquetas podría ser la cabecera de cada porción (Fig. 1.11, izquierda).

Cada nivel maneja una unidad de datos que coincide con la información que le pasa la capa inmediatamente superior junto con las cabeceras que la propia capa inserta para el gobierno de la comunicación con su capa homóloga en el ordenador de destino. En la Fig. 1.11 derecha, se enumeran los nombres específicos que reciben algunas de estas unidades de datos. Cada nivel tiene su propia unidad de datos de protocolo: APDU *(Application Protocol Data Unit)* en el nivel de aplicación, PPDU *(Presentation Protocol Data Unit),* etc.

Los siete niveles de OSI reciben los siguientes nombres de menor a mayor: físico, enlace, red, transporte, sesión, presentación y aplicación.

CEO

SMR_RL_AAbad_01_TiposServiciosOSI.docx

Documento que contiene información sobre:

1. Servicios orientados a la conexión.
2. Servicios sin conexión o de datagramas.

8.2. Niveles OSI orientados a la red

Los niveles inferiores están más próximos a la red, de hecho la capa física se ocupa del hardware. Se dice que las capas física, de enlace y de red están orientadas a la red. Al subconjunto de estas tres capas inferiores se le llama subred.

A. El nivel físico o nivel 1

La capa física se ocupa de definir las características mecánicas, eléctricas, funcionales y de procedimiento para poder establecer y liberar conexiones entre dos equipos de la red. Es la capa de más bajo nivel, por tanto, se ocupa de las transmisiones de los bits expresados como señales físicas.

Ejemplos

Debe garantizar la compatibilidad de los conectores, cuántos pines tiene cada conector y la función de cada uno de ellos, el tipo de sistema de cableado que utilizará, la duración de los pulsos eléctricos, la modulación si la hubiera, el número de voltios de cada señal, el modo de explotación del circuito, etc.

B. El nivel de enlace de datos o nivel 2

La misión de la capa de enlace es establecer una línea de comunicación libre de errores que pueda ser utilizada por la capa inmediatamente superior: la capa de red.

Como el nivel físico opera con bits, la capa de enlace debe fraccionar el mensaje en bloques de datos de nivel 2 o tramas ***(frames).*** Estas tramas serán enviadas en secuencia por la línea de transmisión a través de los servicios de transmisión que ofrece la capa física, y quedará a la escucha de las tramas de confirmación que genere la capa de enlace del receptor.

El nivel de enlace también se ocupará del tratamiento de los errores que se produzcan en la recepción de las tramas, de eliminar tramas erróneas, solicitar retransmisiones, descartar tramas duplicadas, adecuar el flujo de datos entre emisores rápidos y receptores lentos, etc.

Para un estudio más exhaustivo de las funciones de esta capa, es costumbre subdividir esta capa en dos subniveles, repartiendo las funciones entre ellos. Estos subniveles son los siguientes:

- **Subnivel de Control de Acceso al Medio (MAC o *Medium Access Control*).** Este subnivel se encarga de averiguar si el canal de comunicaciones está libre para proceder a efectuar la transmisión. En el caso de que los canales tengan que ser compartidos por múltiples comunicaciones, esta subcapa se encargará del reparto de recursos de transmisión entre todos los nodos de la red, por ejemplo, repartiendo canales, asignando tiempos de uso exclusivo del canal, etc. Obviamente las características de este nivel dependerán del tipo de red, por ejemplo, no es lo mismo acceder al canal guiado de un cable de red, algo típico de las redes cableadas, que el acceso a un canal inalámbrico propio de las redes Wi-Fi. En este subnivel MAC se define la dirección física o dirección MAC, que identifica a cada dispositivo de red unívocamente.
- **Control Lógico de Enlace (LLC o *Logical Link Control*).** En esta capa se sitúan los servicios que gestionan el enlace de comunicaciones, por ejemplo, el control de errores, la formación de las tramas, el control de diálogo entre emisor y receptor y el direccionamiento de la subcapa MAC.

Vocabulario

Encaminamiento o **enrutamiento:** es la técnica por la que se evalúan y deciden las rutas disponibles para transportar un paquete de datos desde su origen en una red hasta su destino en otra red distinta. En la jerga profesional se suele decir «¿por dónde sale el paquete?»

C. El nivel de red o nivel 3

La capa de red se ocupa del control de la subred. La principal función de este nivel es la del **encaminamiento,** es decir, el tratamiento de cómo elegir la ruta más adecuada para que el bloque de datos del nivel de red (paquete) llegue a su destino. Cada destino está identificado unívocamente en la subred por una dirección.

Otra función importante de esta capa es el tratamiento de la congestión. Cuando hay muchos paquetes en la red, unos obstruyen a los otros generando cuellos de botella en los puntos más sensibles. Un sistema de gestión de red avanzado evitará o paliará estos problemas de congestión.

Entre el emisor y el receptor se establecen comunicaciones utilizando protocolos determinados. El mismo protocolo debe estar representado tanto en el emisor como en el receptor.

Un protocolo está en el mismo nivel de red tanto en el emisor como en el receptor. Esto supone que la comunicación en el nivel físico es vista por el nivel de red N como si la comunicación se llevara a cabo mediante un protocolo de comunicación virtual de nivel N. Así por ejemplo, en la capa de red, el emisor interpreta que está utilizando una comunicación mediante un protocolo de red, aunque la única comunicación real es la transmisión física.

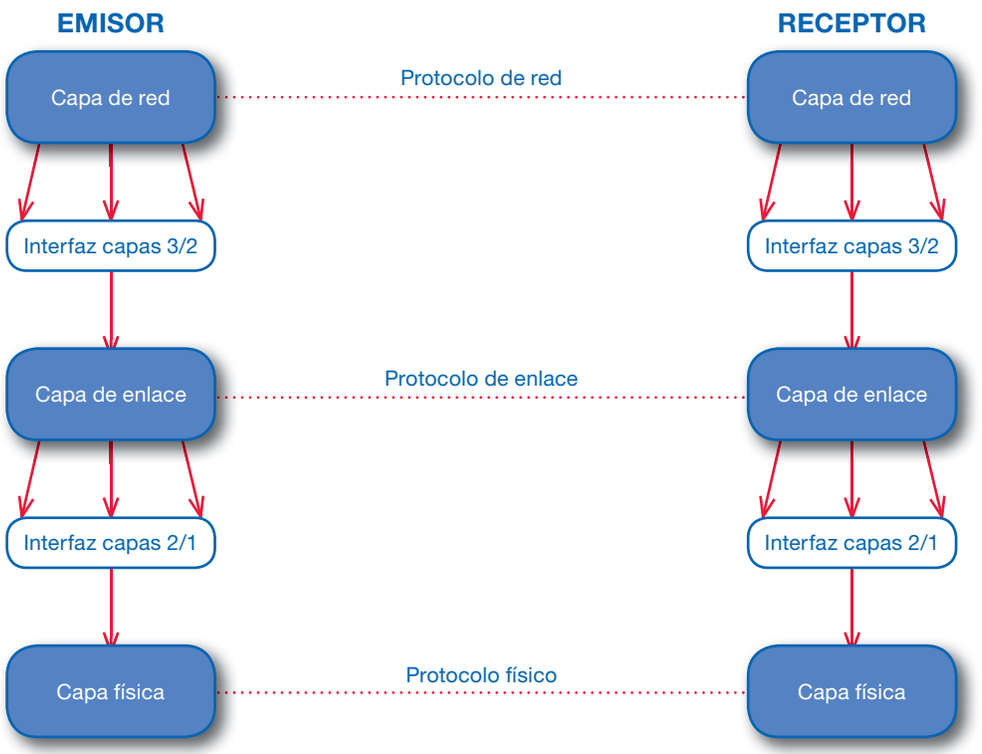


Fig. 1.12. *Modelo de comunicaciones entre capas para los niveles OSI orientados a la red.*

8.3. La capa de transporte

La capa de transporte es una capa de transición entre los niveles orientados a la red (subred) y los niveles orientados a las aplicaciones.

La capa de transporte lleva a cabo las comunicaciones entre ordenadores *peer to peer*, es decir, es el punto en donde emisor y receptor cobran todo su sentido: un programa emisor puede conversar con otro receptor. En las capas inferiores esto no se cumple. Por ejemplo, en el nivel inferior hay transporte de tramas, pero puede ser que para llegar al receptor haya que pasar por varios ordenadores intermedios, que redirijan las comunicaciones o que cambien de red los diferentes paquetes, etc. En el nivel de transporte estos sucesos se hacen transparentes: solo se consideran fuente, destino y tipo de servicio solicitado.

8.4. Niveles OSI orientados a la aplicación

Las capas situadas por encima de este nivel de abstracción del transporte están orientadas a las aplicaciones y, por tanto, la terminología utilizada está exenta de todo lo que tiene que ver con el transporte de datos, se centra más bien en las funciones de aplicación.

A. El nivel de sesión o nivel 5

Esta capa permite el diálogo entre emisor y receptor estableciendo una sesión, que es el nombre que reciben las conexiones en esta capa. A través de una sesión se puede llevar a cabo un transporte de datos ordinario (capa de transporte). La capa de sesión mejora el servicio de la capa de transporte.

B. El nivel de presentación o nivel 6

La capa de presentación se ocupa de la sintaxis y de la semántica de la información que se pretende transmitir, es decir, investiga en el contenido informativo de los datos. Esto es un indicativo de su alto nivel en la jerarquía de capas.

Otra función de la capa de presentación puede ser la de comprimir los datos para que las comunicaciones sean menos costosas, o la de encriptación de la información que garantiza la privacidad de la misma.

Ejemplos

Si el ordenador emisor utiliza el código ASCII para la representación de información alfanumérica y el ordenador receptor utiliza EBCDIC, no habrá forma de entenderse salvo que la red provea algún servicio de conversión y de interpretación de datos. Este es un servicio propio de la capa de presentación.

Ejemplos

Si deseamos transferir un fichero por una línea telefónica que por su excesivo volumen tardará una hora en efectuar el transporte, y la línea telefónica tiene caídas cada quince minutos, será imposible transferir el fichero. La capa de sesión se podría encargar de la resincronización de la transferencia, de modo que en la siguiente conexión se transmitieran datos a partir del último bloque transmitido sin error.

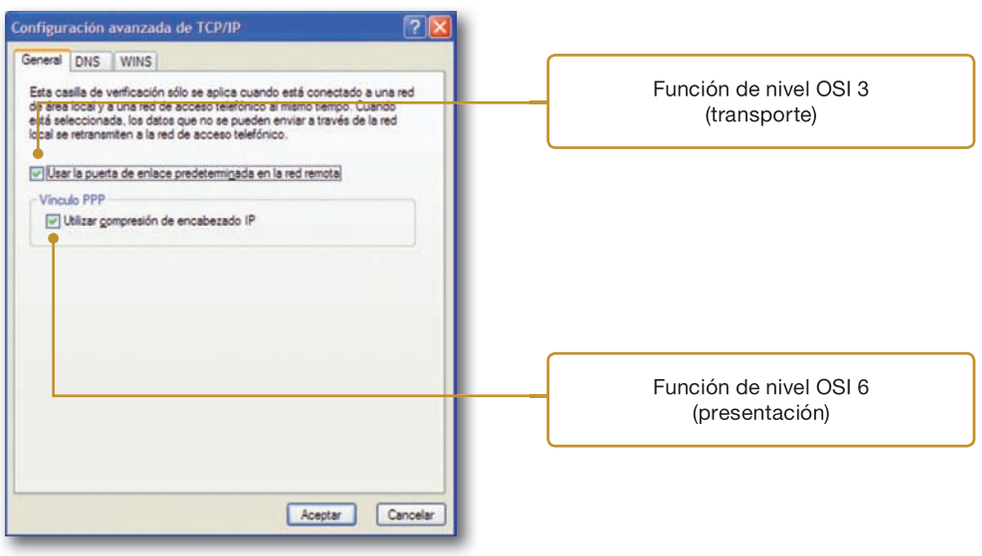


Fig. 1.13. Ficha de configuración para que una transmisión de datos por teléfono comprima las cabeceras del protocolo PPP, servicio típico del nivel de presentación en el modelo de red OSI. La elección de la puerta de enlace es una función utilizada por la capa 4 de red, que deberá ser resuelta por el nivel 3.

C. El nivel de aplicación o nivel 7

Es la capa superior de la jerarquía OSI. En esta capa se definen los protocolos que utilizarán las aplicaciones y procesos de los usuarios. La comunicación se realiza utilizando protocolos de diálogo apropiados. Cuando dos procesos que desean comunicarse residen en el mismo ordenador utilizan para ello las funciones que le brinda el sistema operativo. Sin embargo, si los procesos residen en ordenadores distintos, la capa de aplicación disparará los mecanismos necesarios para producir la conexión entre ellos, sirviéndose de los servicios de las capas inferiores.

Si un usuario de la red quiere comunicarse con otro en la misma o distinta red, elegirá un sistema de comunicación concreto sobre el que pueda intercambiar mensajes. Por ejemplo, podría hacerlo mediante el correo electrónico o a través de un sistema de mensajería electrónica instantánea; también podría elegir una aplicación de transmisión de voz; si tuviera que transmitir información gráfica podrían compartir una pizarra digital, etc. Cada uno de estos sistemas utilizará su propio conjunto de protocolo de aplicación de nivel *7*.

El concepto de aplicación a que se refiere esta capa no es el mismo que el de utilidad de software. En comunicaciones se entiende por aplicación a un modo específico de comunicarse. Por ejemplo, una aplicación es el correo electrónico, otro es la carga/descarga de ficheros, otra la consulta de una página web, etc.

Cada una de estas aplicaciones da origen a uno o varios protocolos (habitualmente una familia de protocolos) del nivel *7*. Por ejemplo, los protocolos SMTP, POP e IMAP constituyen una familia de protocolos de nivel de aplicación para la gestión del correo electrónico (servidores de correo), HTTP es un protocolo de nivel *7* para uso de la web (servidor web), FTP es el protocolo de aplicación específico para la carga y descarga de ficheros (servidor FTP), etc. Es evidente que el número de protocolos de nivel *7* es muy elevado y no deja de crecer: cada aplicación nueva requiere los protocolos indispensables para su funcionamiento. En las siguientes unidades se irán describiendo algunos de estos protocolos de uso frecuente.

Por otra parte, las aplicaciones de software que manejan los usuarios de los servicios de red se corresponden con estos protocolos de nivel de aplicación. Por ejemplo, un programa que lea y envíe correos electrónicos tendrá que ser capaz de manejar SMTP, POP e IMAP, un navegador web tendrá que utilizar el protocolo HTTP y así sucesivamente.

Laboratorio

Comprensión de algunos procesos sobre protocolos de red

En las siguientes páginas puedes encontrar animaciones que te ayudarán a aclarar algunos conceptos relacionados con los protocolos y la arquitectura OSI.

Visualiza cada página, intenta comprender cómo funciona y describe brevemente el funcionamiento del proceso que representa. Para realizar un buen trabajo puede que tengas que completar la información utilizando un buscador de páginas web.

- **http://www.iesjuanantoniocastro.es/Profesores/JASORTIZ/Archivos/Flashes/FlashFOR-Anillo.swf**
- **http://www.iesjuanantoniocastro.es/Profesores/JASORTIZ/Archivos/Flashes/FlashCisco-CapasOSI.swf**
- **http://www.iesjuanantoniocastro.es/Profesores/JASORTIZ/Archivos/Flashes/FlashFOR-IntercambioOSI.swf**
- **http://www.iesjuanantoniocastro.es/Profesores/JASORTIZ/Archivos/Flashes/FlashCisco-EncapsulamientoOSI.swf**
- **http://www.iesjuanantoniocastro.es/Profesores/JASORTIZ/Archivos/Flashes/FlashFOR-ColisionCSMA-CD.swf**

Actividades

17. Si OSI es un modelo de arquitectura que no se utiliza comercialmente, ¿por qué es tan importante conocer este modelo con cierta profundidad?

18. ¿Cómo se llaman los siete niveles OSI?

19. Describe una característica concreta de cada uno de los niveles OSI.

20. ¿Qué es una trama de red? ¿Y un paquete de red? ¿Y una N-PDU?

Ejemplos

Analogía del modelo OSI con una operación de distribución logística

Este ejemplo pretende describir con la mayor precisión las funcionalidades de los niveles OSI con una analogía de la actividad humana ordinaria. El ejemplo consistirá en descomponer en fases el transporte de una mercancía desde el lugar de producción hasta el lugar de venta. Supongamos que una cooperativa agrícola tiene como cliente habitual un mercado de abastos de fruta situado en una ciudad de otro país. Las frutas deben ser recogidas en la cooperativa y trasladadas al mercado de abastos. Vamos a descomponer el proceso de transporte tal y como es visto por la cooperativa clasificando los eventos producidos por analogía en las diferentes capas de OSI. Los datos que aparecerán, aunque son orientativos y tienen un fin exclusivamente didáctico, pueden sernos útiles para clarificar los conceptos abstractos.

	Eventos	Observaciones
Nivel 7 o de aplicación	La cooperativa recoge los frutos que aportan los agricultores, negocia un precio de venta con el mercado de abastos y decide proceder al transporte de la mercancía.	Este evento está en contacto directo con los usuarios de la comunicación: el comprador y el vendedor. La aplicación sería una operación comercial de compraventa, que no se puede llevar a cabo sin un fenómeno de transporte.
Nivel 6 o de presentación	Una vez recogidas las frutas deben empaquetarse y presentarse como cestas con un peso bruto determinado. Además, hay que colocar las cestas de modo que ocupen un espacio mínimo con el fin de facilitar el transporte. Las cajas con las cestas van precintadas.	Este evento se ocupa de que las frutas tengan un aspecto (presentación) determinado cara al consumidor. Además, lleva incorporado un proceso de compresión para facilitar el transporte. El precinto de cada caja sirve de encriptación, hace que la carga tenga privacidad.
Nivel 5 o de sesión	El comprador y el vendedor se ponen de acuerdo para enviar todos los lunes, miércoles y viernes 10 toneladas de fruta, sin embargo, la semana que viene habrá una excepción: el viernes es festivo y la fruta se transportará en lunes, miércoles y jueves. Los pagos se harán con letras de cambio con un vencimiento a treinta días.	En este evento se abre una sesión en la que se especifica cómo serán los envíos, es decir, se establece el diálogo sobre cómo proceder para efectuar el transporte. Además se negocia el sistema de pago.
Nivel 4 o de transporte	Ya es lunes. Hoy hay que efectuar un transporte de fruta. Llamamos a la compañía de transportes para que recoja la fruta. Se compromete a entregarla en el mercado de abastos en el plazo fijado de antemano y en las debidas condiciones de salubridad. Comprueba que el terminal de descarga del mercado de abastos tiene previsto que llegará una carga de fruta de diez toneladas en pocas horas.	En este evento se efectúa una conexión. Se negocia la calidad de servicio con parámetros como el plazo de entrega de la carga, el buen estado de la misma, etc. Para cumplir el plazo de entrega la capa inmediatamente inferior deberá elegir medios de comunicación apropiados, suficientemente rápidos (avión o vías terrestres amplias y poco congestionadas, etc.). Además, comprueba que el destinatario puede ofrecer este servicio: en el mercado hay un lugar para la fruta.

Continúa…

Ejemplos

... Continuación

	Eventos	Observaciones
Nivel 3 o de red	La compañía de transportes determina las rutas posibles para efectuar el traslado de la carga, así como la tecnología de transporte más adecuada. Elige el siguiente sistema: cinco toneladas viajarán en avión y las otras cinco toneladas por carretera en camión. Además se decide el rumbo que debe seguir el avión para evitar una zona de borrasca y las carreteras apropiadas para evitar atascos de tráfico. La carga que irá en avión debe empaquetarse en un contenedor especial para la bodega del avión. La carga que viaja por carretera se empaqueta en cajas de cartón acinturadas con plástico. Tanto el contenedor aéreo como cada una de las cajas llevan adheridas las etiquetas que identifican al aeropuerto de destino, o la dirección del terminal de descarga destinatario.	En este evento se estudian las rutas. A partir de esta capa ya se tienen en cuenta las tecnologías físicas o lógicas de bajo nivel que serán utilizadas para producir el fenómeno de transporte. Se seleccionan las rutas más adecuadas. Hay un fraccionamiento de la carga por necesidades del servicio de transporte. La carga se encapsula de un modo apropiado para la tecnología de transporte. Cada unidad de carga (contenedor o caja) lleva la dirección de origen y destino (aeropuerto o mercado, que es donde llegan los medios de transporte). Además, las rutas han sido elegidas de acuerdo con ciertos criterios de eficacia: poca congestión de tráfico, mejora en las condiciones de vuelo, etc.
Nivel 2 o de enlace	Al contenedor de avión se le añade un control de seguridad, se observa que tiene un peso excesivo y se reparte en dos contenedores más pequeños. Se instalan uno a cada lado de la bodega de la aeronave para distribuir proporcionalmente la carga. A la otra mitad de la carga, la que viaja por carretera, se la distribuye en diez camiones frigoríficos. Cada uno se precinta por seguridad. Cada unidad de carga lleva su etiquetado de origen y destino. Cada camión registra la temperatura habida en el viaje. Si no es la prevista, el termómetro del camión frigorífico servirá de prueba para declarar inservible la carga y pedir una nueva carga.	En este evento se expresa el equivalente a los controles de errores: el termómetro, los precintos de seguridad, etc. La carga ha de repartirse para hacer posible el transporte en ese avión concreto en el que viajará o en los camiones frigoríficos, que tienen una tara y un peso máximo autorizado, es decir, debemos ajustarnos a la tecnología concreta de bajo nivel que se utilizará. Si se ha producido error se pedirá una devolución y reposición de la carga (retransmisión).
Nivel 1 o físico	Tanto el avión por vía aérea como los camiones por vía terrestre, transportarán la carga al lugar de destino.	Aquí es donde se produce realmente el transporte de la carga.

9. Elementos de la red

Con este epígrafe vamos a terminar de componer el mapa de conocimientos necesarios para el técnico de redes. Ya se ha estudiado la necesidad de la red y los problemas que viene a resolver, los estándares a los que se acogen estas redes, sus tipos y topologías. Nos falta por completar una lista con los elementos que componen estas redes y que se irán estudiando con detalle en las siguientes unidades.

9.1. El cableado, la conectorización y los espacios en los que se localiza físicamente la red

Es el elemento más específico de la red aunque en ocasiones, como en el caso de las redes inalámbricas, es inexistente y se sustituye por antenas de radiación.

El cableado puede ser de cobre o de fibra óptica, pero no solo nos hemos de fijar en los cables, sino también en los conectores. No todos los conectores pueden ser terminadores de cualquier cable. Cada tipo de cableado lleva su propio sistema de conectorización.

9.2. Los dispositivos específicos de red

Son máquinas altamente especializadas en alguna función de red. Algunos de estos dispositivos trabajan en alguno de los niveles de red, pero otros absorben funciones de más de una capa.

Entre estos dispositivos están los módems para realizar conexiones remotas mediante líneas telefónicas, concentradores y repetidores para regenerar la señal eléctrica en distintos segmentos de red, conmutadores para el intercambio selectivo de tramas de datos entre diferentes segmentos de la red, encaminadores para transportar paquetes entre redes y, por último, las pasarelas, que son los dispositivos que operan en los niveles más altos de OSI. Algunos ejemplos de pasarelas podrían ser los dispositivos de filtrado de contenidos de Internet, analizadores de antivirus, pasarelas de telefonía, cortafuegos, analizadores de intrusiones, etc.

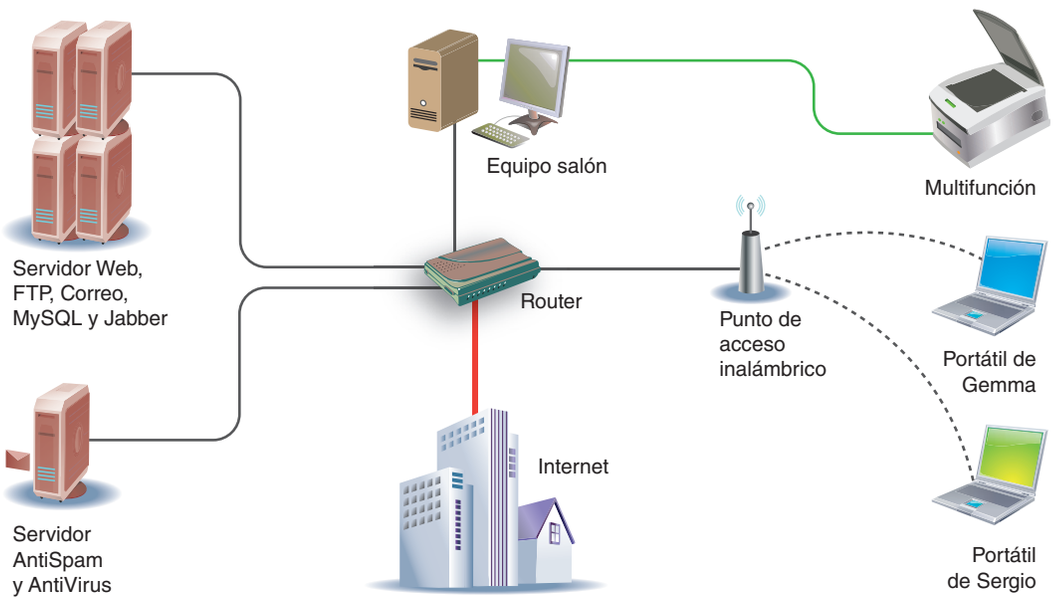


Fig. 1.14. *Esquema de una red doméstica real en la que se significan los diferentes elementos de la red.*

Ampliación

El sistema de cableado tiene que recorrer los recintos sobre los que se ubican los ordenadores que deben comunicarse entre sí. Esto define un conjunto de espacios, armarios y cuartos de comunicaciones en los que se instalan algunos dispositivos de red especializados y se practica parte de la conectorización estructurando el sistema de cableado.

Vocabulario

Por extensión, **nodo** en Telemática suele atribuirse a cualquier dispositivo activo conectado a una red. El término **host** suele asociarse a un nodo que aloja un servicio de red y que es proporcionado a los clientes a través de la red a la que se conecta, por ello, un host siempre es un nodo. Por ejemplo, son nodos las estaciones cliente, los servidores, los encaminadores, etc.

9.3. Nodos de la red

Los nodos pueden estar conectados a la red mediante cable o de modo inalámbrico. Cada nodo requiere al menos una interfaz de red que es soportada mediante una tarjeta de red o, de un modo más general, algún dispositivo físico sobre el que pueda interactuar el software de la red. Estas tarjetas o dispositivos de red deberán poseer la interfaz apropiada para la conexión del cable o antena que una el nodo al resto de la red.

9.4. Software de red

Todos los dispositivos activos en la red tienen que ejecutar operaciones informáticas avanzadas para cumplir lo establecido por los protocolos de red, por lo que tienen que tener una cierta capacidad de proceso conducida por el software correspondiente. A este software se le denomina software de red.

En el estadio superior se sitúan las aplicaciones que proporcionan los servicios avanzados de la red, aunque estas aplicaciones se proporcionan frecuentemente por los sistemas operativos: correo electrónico, mensajería electrónica, software de colaboración y publicación electrónica, etc. En este nivel se encuentran los programas cliente que manejan directamente los usuarios de la red.

Algunas otras aplicaciones que se utilizan en diferentes niveles son los gestores de red, los recopiladores de estadísticas, analizadores de congestión, etc.

Ampliación

Este software de red puede ser muy variado. En el nivel inferior se posicionan los controladores de los interfaces de conexión, por ejemplo, de las tarjetas de red o de los módems. Por encima de este software se debe ejecutar la parte del sistema operativo que provee los servicios básicos de comunicación: confección de tramas, recuperación de errores, direccionamiento de red, encaminamiento, etc.

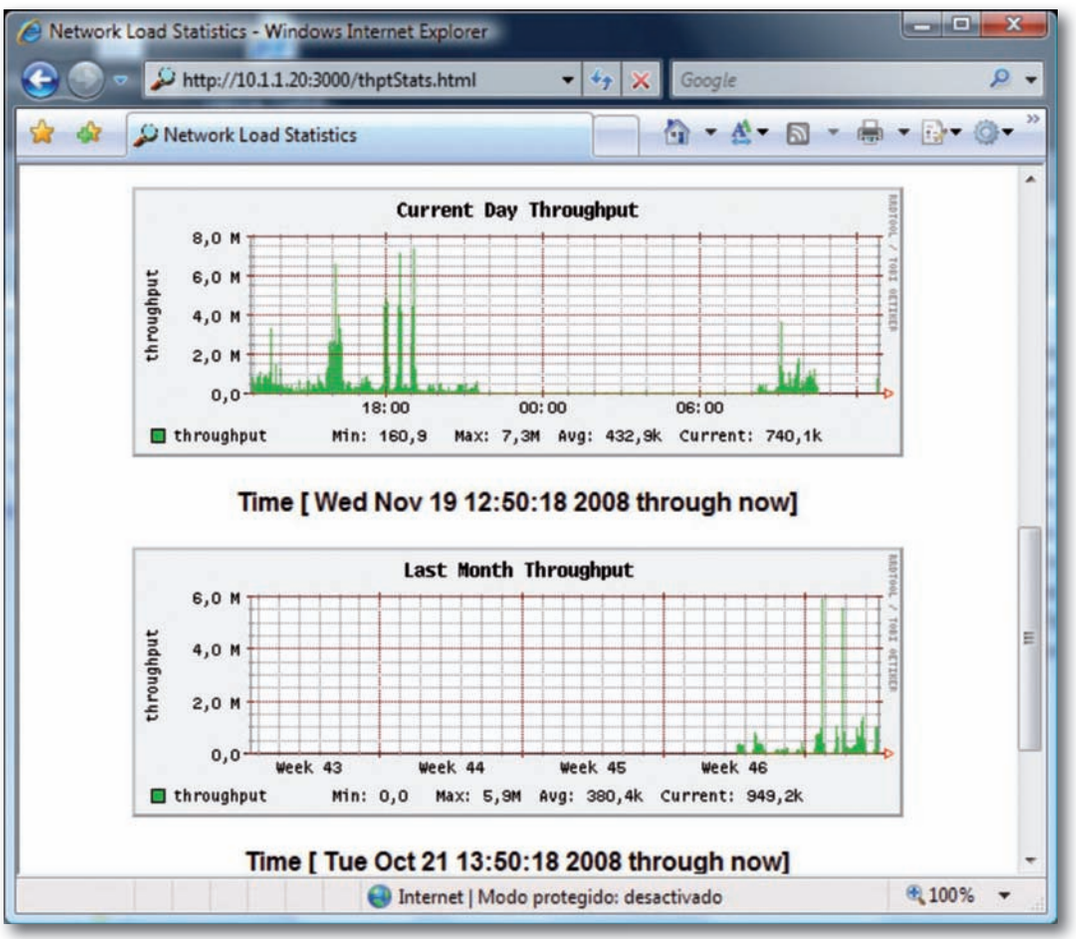
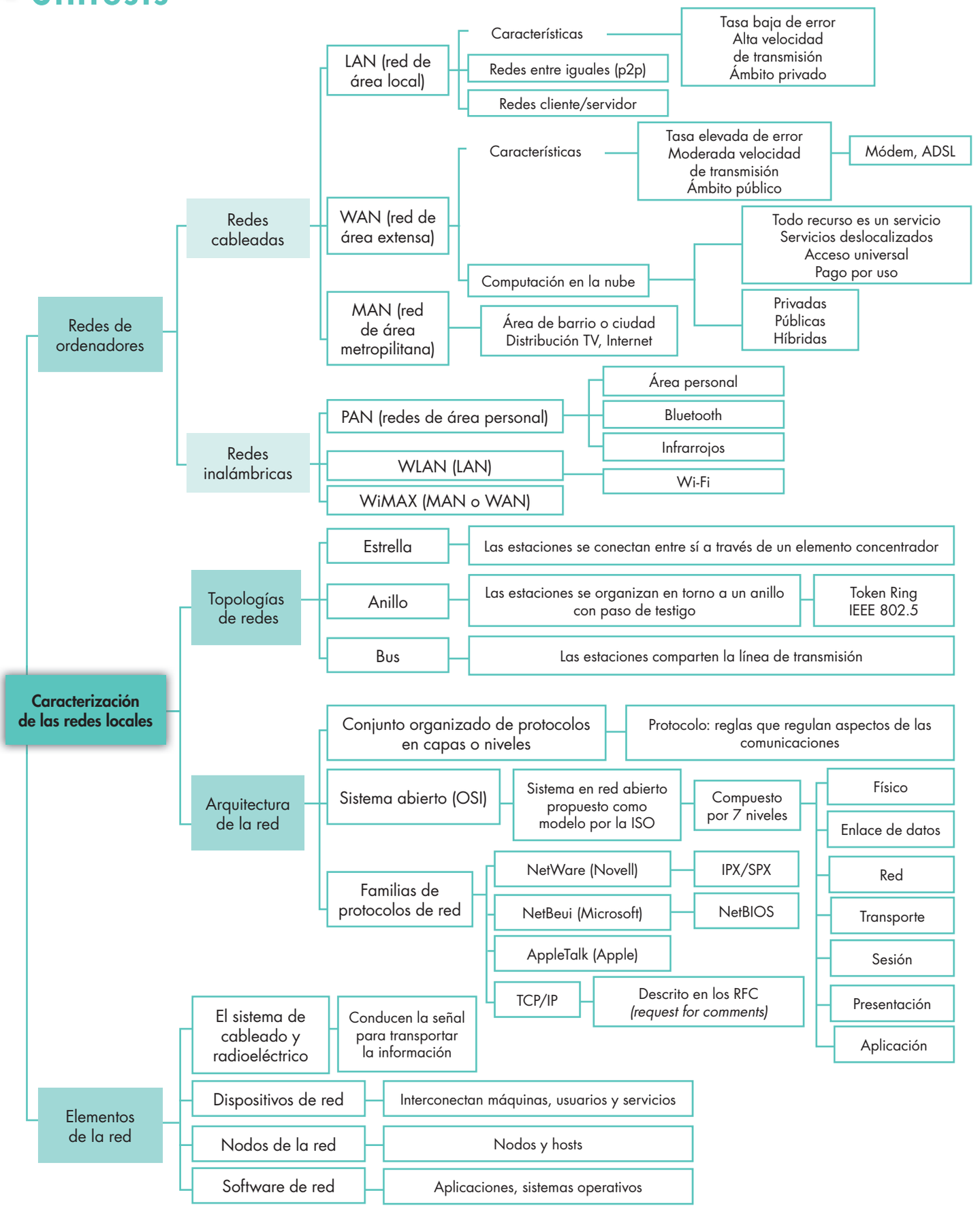


Fig. 1.15. *Gráficos proporcionados por NTOP, una aplicación de uso libre para gestionar las estadísticas de tráfico de red.*

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de distintos tipos de redes:

a) LAN	1) Entorno mundial	i) Entorno público
b) WAN	2) Red doméstica	ii) Difusión de TV
c) MAN	3) Entorno de una ciudad	iii) Entorno privado
d) PAN	4) Entorno de un edificio u oficina	iv) Bluetooth

2. Las redes entre iguales:

a) Necesitan un servidor central.

b) Posibilitan los accesos cruzados entre todos los nodos de la red.

c) Requieren ordenadores con el mismo sistema operativo.

d) Solo se pueden utilizar en Internet.

3. Enlaza los siguientes elementos característicos de distintos tipos de redes:

a) WLAN	1) Servicios distribuidos y deslocalizados	i) Acceso universal
b) Nube	2) LAN inalámbrica	ii) Cloud computing
c) Internet	3) WAN	iii) Wi-Fi

4. La topología de una red en estrella requiere:

a) Un nodo central.

b) Un anillo central.

c) Un bus de comunicaciones común a todas las estaciones.

d) Un nodo central y un bus común.

5. Enlaza los siguientes elementos característicos sobre familias de protocolos:

1. NetWare	a. Internet	i. NWLink
2. NetBeui	b. NetBIOS	ii. IBM y Microsoft
3. TCP/IP	c. IPX/SPX	iii. RFC

6. La capa física del modelo OSI:

a) Se encarga de confeccionar las tramas.

b) Especifica cómo son las señales eléctricas en los cables.

c) Describe cómo encaminar los paquetes a su destino.

d) Cifra y descifra los datos enviados.

7. Las pasarelas son dispositivos de la red que:

a) Operan en el nivel más alto del modelo de red OSI.

b) Intercambian tramas entre otras dos estaciones de la red.

c) Regeneran la señal eléctrica en los sistemas de cableado de la red.

d) Comunican distintos segmentos de la red.

8. ¿Cuáles de las siguientes afirmaciones son verdaderas?

a) Los nodos de la red se conectan siempre mediante cables.

b) Los nodos requieren de una interfaz de red para conectarse a la misma.

c) Una estación se puede conectar inalámbricamente, pero un nodo no.

d) Un nodo puede tener más de una tarjeta de red.

9. El nivel 3 del modelo de red propuesto por OSI:

a) Se ocupa de la sintaxis de los mensajes transmitidos.

b) Define los protocolos de red utilizados por las aplicaciones de los usuarios.

c) Se encarga del encaminamiento de los paquetes.

d) Detecta los problemas que surgen en la transmisión eléctrica del cable.

10. Un protocolo de red es:

a) La interfaz entre dos capas consecutivas en la arquitectura de red.

b) El conjunto organizado de capas.

c) Un sistema abierto.

d) Un conjunto de reglas que regulan algún aspecto de una comunicación.

Solución: 1: a-4-iii, b-1-i, c-3-ii, d-2-iv; **2:** b; **3:** a-2-iii, b-1-ii, c-3-i; **4:** a; **5:** a-3-i, b-2-ii, c-1-iii; **6:** b; **7:** a; **8:** son verdaderas b y d; **9:** c; **10:** d.

Comprueba tu aprendizaje

I. Conocer las fuentes de información de estándares

1. Consulta las sedes web de las asociaciones de estándares más importantes y elabora una jerarquía de carpetas de hiperenlaces URL favoritos a las páginas de mayor interés, de novedades, de recursos, etc.

   Puedes añadir estos hipervínculos a tu carpeta de favoritos del explorador de Internet que uses habitualmente porque los utilizarás con frecuencia.

2. Busca en Internet información sobre los RFC de los protocolos SMTP, POP e IMAP que son utilizados por las aplicaciones de gestión de correo electrónico. ¿En qué números de RFC se detallan estos protocolos?

II. Identificar los distintos tipos de redes

3. Clasifica las redes que intervienen en las circunstancias que se citan a continuación según sean PAN, WAN, LAN, MAN, WLAN o *cloud computing*. Razona la respuesta.

   a) Una conexión por módem a Internet.

   b) Un televisor recibe una transmisión televisiva por cable.

   c) Un receptor de radio recibe por su antena la radiodifusión de un programa musical.

   d) Un ordenador se conecta a una red para imprimir por una impresora de red.

   e) Una agenda electrónica sincroniza el correo electrónico utilizando Bluetooth.

   f) Varios usuarios comparten una conexión a Internet sin necesidad de cables.

   g) Dos campus universitarios en la misma ciudad, pero distantes, se conectan mediante fibra óptica.

   h) Una aplicación accede a sus datos en Internet desde cualquier lugar.

4. A continuación se va a especificar un conjunto de palabras, siglas y acrónimos. Se trata de que relaciones cada uno de ellos con los distintos tipos de redes. Razona la respuesta.

   a) Wi-Fi.

   b) Ethernet.

   c) Frame-Relay.

   d) X.25.

   e) Token Ring.

   f) Ondas de radio.

   g) WiMAX.

   h) Bluetooth.

5. Describe los factores que harían necesaria la introducción de una red de área local en el flujo de trabajo de una oficina bancaria. Se propone la discusión de resultados en una tormenta de ideas.

III. Identificar los distintos elementos de una red

6. De los elementos que se enumeran a continuación, di cuáles son dispositivos activos de interconexión de red y cuáles no. Razona la respuesta.

   a) Encaminador.

   b) Punto de acceso inalámbrico.

   c) Cable coaxial.

   d) Conmutador.

   e) Armario de comunicaciones.

   f) Disco duro.

   g) Sistema operativo de red.

   h) Módem.

   i) Conexión ADSL.

   j) Router ADSL.

7. Dibuja con una aplicación informática de tratamiento de gráficos un ejemplo hipotético de red en el que aparezcan clientes, servidores, algunos dispositivos de red que interconecten clientes con servidores, un encaminador para la conexión a Internet, un punto de acceso inalámbrico y varios clientes inalámbricos.

   Identifica cada elemento del gráfico con su correspondiente rótulo. En los nodos de red con sistema operativo añade en un rótulo qué sistema operativo debe llevar.

IV. Reconocer las distintas topologías de red

8. Averigua si son verdaderas o falsas las siguientes afirmaciones:

   a) Una red en anillo es más rápida que una red en bus.

   b) Una red en bus en más rápida que una red en anillo.

   c) La rotura del anillo de una red impide totalmente la comunicación en toda la red.

Comprueba tu aprendizaje

d) La rotura de un segmento de red en una red en árbol impide la comunicación en toda la red.

e) Una red en bus es muy sensible a la congestión provocada por exceso de tráfico.

f) Una red en bus se adapta mejor a la estructura de cableado de un edificio.

g) Una red en anillo se adapta mejor a la estructura de un campus.

h) Todas las redes metropolitanas son anillos.

9. Utilizando como herramienta una aplicación de gráficos, dibuja un ejemplo de cada tipo de topología que conozcas. Después indica algunas analogías y diferencias entre esas topologías.

10. Sobre las redes diseñadas en el ejercicio anterior, propón algún ejemplo concreto de instalación para cada una de esas topologías.

    Comenta estas ideas en grupo para contrastar las diferentes opiniones que se manifiesten.

    Descubrirás que aunque hay topologías que se prestan más que otras a algunas circunstancias, no se puede afirmar rotundamente que a cada topología le corresponda un tipo de instalación.

V. Conocer la composición de la arquitectura de red estándar OSI

11. Realiza un gráfico que describa la estructura de siete niveles de la arquitectura OSI para redes de ordenadores. Escribe en cada capa el nombre que la identifica y agrúpalas en función de que estén orientadas a la red o al usuario.

12. Imagina una estructura en forma de capas, semejante a la realizada en el texto para la cooperativa agrícola, que describa un proceso de distribución de prensa escrita.

    Algunos elementos que puedes considerar a la hora de estructurar las operaciones de logística de prensa escrita en capas son los siguientes:

    a) Los periódicos deben estar impresos a cierta hora.

    b) Se agrupan formando paquetes.

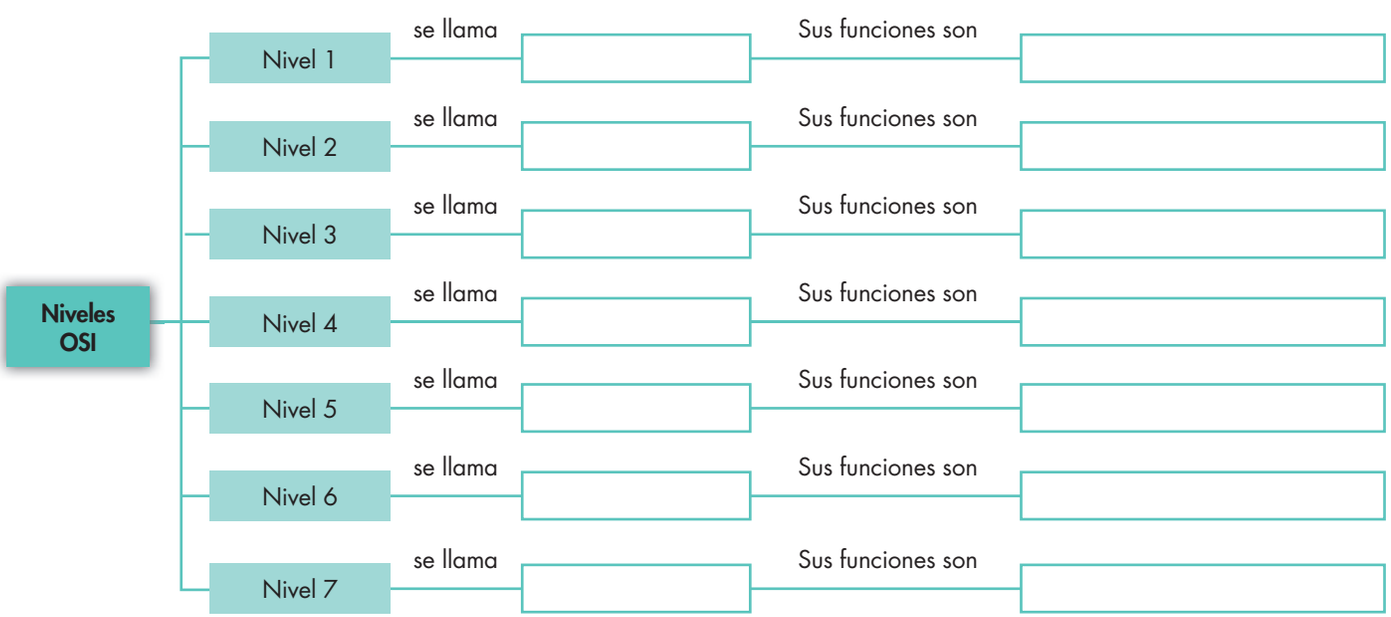
    c) El etiquetado de los paquetes de periódicos describe los destinos y las rutas de transporte.

    d) Los camiones que transportan estos paquetes tienen como destino ciudades.

    e) La distribución a quioscos o puntos de venta se realiza en furgonetas desde la central de transporte de la ciudad.

    f) Se puede considerar el proceso de devolución de periódicos no vendidos.

13. Consolida la nomenclatura de cada una de las capas OSI rellenando en el siguiente mapa conceptual las cajas que aparecen en blanco con los nombres de las capas y las funciones fundamentales de cada una de ellas.



Unidad 2

La instalación física de una red

En esta unidad aprenderemos a:

- Identificar los espacios físicos de la red documentándolos con aplicaciones gráficas.
- Desplegar el sistema de cableado de una red local.
- Montar los sistemas de conectorización de la red.
- Adquirir buenas prácticas profesionales en instalaciones, seguridad laboral y en el cuidado del medioambiente.

Y estudiaremos:

- Los medios de transmisión utilizados en redes y los distintos tipos de conectores.
- Los modos de estructuración del cable.
- Alguna utilidad gráfica que te permita documentar la red.
- Las herramientas para la conectorización y la certificación del cableado.

Claves y consejos

La elección de un buen sistema de cableado es de vital importancia en las instalaciones reales en las que se producirá el fenómeno de la comunicación. La inversión estimada para cables en una instalación es inferior al 10 % del coste total. Sin embargo, está comprobado que el 70 % de los fallos producidos en una red se deben a defectos en el cableado. Por tanto, merece la pena no escatimar demasiado las inversiones que deban producirse en los sistemas de transmisión.

CEO

SMR_RL_AAbad_02_LeyOhm.docx

Documento que contiene información sobre la ley de Ohm para conductores.

Truco

Es mucho más fácil instalar cable UTP que STP debido a que STP, al estar apantallado, es mucho menos flexible, lo que a veces dificulta el tendido del cable. Además, las mallas protectoras de los cables STP deben estar conectadas a tierra, lo que multiplica el trabajo.

1. Los medios de transmisión

Nos ocuparemos en esta unidad del nivel físico de la red, es decir, de las funciones y especificaciones de la primera capa del modelo de referencia OSI. Sin embargo, la instalación de red no solo implica cables y conectores. La red debe extenderse por la instalación de una vivienda o una oficina, lo que hace que el despliegue del sistema de cableado sea más complejo que la simple confección de los cables por donde viajará la señal de red.

El medio de transmisión es el soporte físico que facilita el transporte de la información y supone una parte fundamental en la comunicación de datos. La calidad de la transmisión dependerá de sus características físicas, mecánicas, eléctricas, etc.

El transporte, según hemos visto, puede ser mecánico, eléctrico, óptico, electromagnético, etc. El medio debe ser adecuado para la transmisión de la señal física con objeto de producir la conexión y la comunicación entre dos dispositivos.

1.1. Los cables de pares y metálicos

Vamos a incluir en este apartado todos los medios de transmisión que utilizan canales conductores metálicos para la transmisión de la señal, y que están sujetos tanto a la ley de Ohm, como a las leyes fundamentales que rigen el electromagnetismo.

Los cables de pares están formados por pares de filamentos metálicos y constituyen el modo más simple y económico de todos los medios de transmisión. Sin embargo, presentan algunos inconvenientes: cuando se sobrepasan ciertas longitudes, hay que acudir al uso de repetidores para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, si no están apantallados, son muy sensibles a interferencias y diafonías producidas por la inducción electromagnética de unos conductores en otros (motivo por el que en ocasiones percibimos conversaciones telefónicas ajenas en nuestro teléfono).

Un modo de subsanar estas interferencias consiste en trenzar los pares de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos. Esta es la razón por la que este tipo de cables se llaman cables de pares trenzados. Existen fundamentalmente dos tipos:

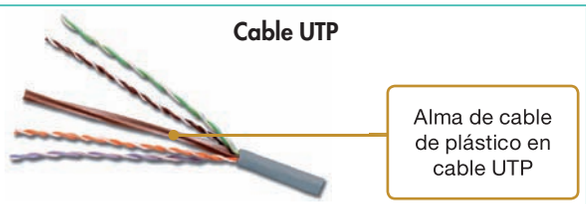
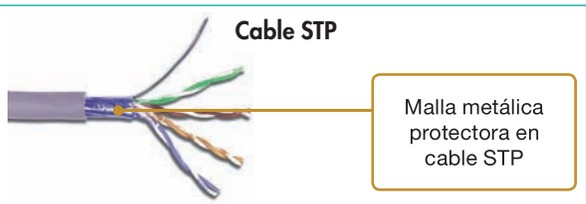
Cable UTP  	UTP son las siglas de *Unshielded Twisted Pair*. Es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz disminuyendo sensiblemente o incluso impidiendo la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar.
Cable STP  	STP son las siglas de *Shielded Twisted Pair*. Este cable es semejante al UTP pero se le añade un recubrimiento metálico para evitar las interferencias externas. Este recubrimiento debe ser conectado a la tierra de la instalación. Por tanto, es un cable más protegido, pero menos flexible que el UTP. El sistema de trenzado es idéntico al del cable UTP.

Tabla 2.1. *Ejemplos de cables de pares.*

Obviamente, el cable STP tiene más ventajas eléctricas que el cable UTP por lo que, en principio, siempre se tendría que elegir STP en vez de UTP, sin embargo, la falta de flexibilidad originada por su rigidez hace que solo se utilice en donde realmente hace falta: en entornos eléctricamente hostiles.

En los cables de pares hay que distinguir dos clasificaciones:

- Primera clasificación: las **categorías.** Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia. Las categorías 3 a 5, que soportan frecuencias de 10, 20 y 100 MHz respectivamente, empiezan a estar en desuso, sin embargo, es frecuente encontrarlas instaladas en instalaciones antiguas. También se utiliza una categoría llamada 5e, que mejora algo las capacidades de la categoría 5. Las categorías 6 (estándar ANSI/TIA/EIA-568-B.2-1) y 7 (categoría ISO/IEC 11801:2002 categoría 7/clase F) llegan a transmisiones de 250 y 600 MHz respectivamente. El estándar que define estas categorías es el TIA/EIA-568-B. Actualmente lo más frecuente es instalar categoría 5e o 6.
- Segunda clasificación: las **clases.** Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características. Están detalladas las clases A a F. En la Tabla 2.2 se especifican ejemplos que relacionan algunas clases con algunas categorías. Para las categorías superiores los parámetros dependerán mucho del entorno de operación.

CLASES	Clase A	Clase B	Clase C	Clase D	Clase E	Clase F
Ancho de banda	100 KHz	1 MHz	20 MHz	100 MHz	250 MHz	600 MHz
Cat. 3	2 km	500 m	100 m	No hay	No hay	No hay
Cat. 4	3 km	600 m	150 m	No hay	No hay	No hay
Cat. 5	3 km	700 m	160 m	100 m	No hay	No hay
Cat. 6	Sin uso	Sin uso	Sin uso	Sin uso	1 Gbps	No hay
Cat. 7	Sin uso	Sin uso	Sin uso	Sin uso	Sin uso	10 GBps

Tabla 2.2. *Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados.*

Investigación

Las especificaciones sobre cableados contienen una información técnica muy compleja característica del diseño de ingeniería. No obstante, conviene leer algunos documentos sobre ellos para conocer qué elementos tecnológicos contienen. Se sugiere leer las páginas de Wikipedia relativas a las siguientes voces: «Unshielded Twisted Pair»», «Shielded Twisted Pair», «TIA-568B», «Cable de Categoría 6» y «Cable de Categoría 7». Pásate también por la sede web de Lanshack **(http://www.lanshack.com),** que es un proveedor de sistemas de cableado para inspeccionar el catálogo de productos y hacerte una idea de los precios de cada componente. En **http://www.lanshack.com/cat5e-tutorial.aspx** tienes un tutorial muy completo, aunque en inglés, sobre los cables de categoría 5 y 6.

Dado que el cable UTP de categorías 5 y 5e es barato y fácil de instalar, se utiliza habitualmente en las instalaciones de redes de área local con topología en estrella, mediante el uso de conmutadores y concentradores que estudiaremos más adelante.

Las aplicaciones típicas de la categoría 3 son transmisiones de datos hasta 10 Mbps (por ejemplo, la especificación 10BaseT); para la categoría 4, 16 Mbps y para la categoría 5, 100 Mbps (por ejemplo, la especificación 100BaseT).

En concreto el cable UTP de categoría 5 viene especificado por las características de la Tabla 2.3 referidas a un cable estándar de cien metros de longitud.

Velocidad de transmisión de datos	Nivel de atenuación para 100 m
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

Tabla 2.3. *Nivel de atenuación permitido según la velocidad de transmisión para un cable UTP de categoría 5 de 10 m de longitud.*

Las sociedades de estándares han hecho evolucionar la categoría 5 definiendo otras de características mejoradas que se describen a continuación:

- **Categoría 5.** Se define en los estándares IS 11801, EN 50173 y TIA 568. En su versión original data de 1995 y está pensado para soportar transmisiones típicas de la tecnología ATM (155 Mbps), pero no es capaz de soportar Gigabit Ethernet (1 Gbps).
- **Categoría 5 mejorada** (5e o *5 enhanced*). Se trata de una revisión de la categoría 5 de 1998. En esta versión se mejoran los parámetros del cable para llegar a transmisiones de Gigabit Ethernet.
- **Categoría 6.** Es una categoría ya ampliamente aceptada. Soporta frecuencias hasta los 250 MHz en clase E. Es la tecnología que poco a poco va sustituyendo a la 5e.
- **Categoría 7.** Llega hasta los 600 MHz en clase F, mejorando sustancialmente los fenómenos de diafonía con respecto de la categoría 5. Sin embargo, esta categoría tiene como competidor más directo a la fibra óptica.

Para hacernos una idea aproximada de la utilización de estos cables en redes de área local podemos afirmar que típicamente se puede construir una red Ethernet con topología en estrella con cable UTP de categoría 5e utilizando segmentos de 100 m como máximo.

CEO

SMR_RL_AAbad_02_CableCoaxial.docx

Documento que contiene información sobre características técnicas de los cables coaxiales.

Ampliación

Es posible efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra dado su gran ancho de banda. Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a los cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas en el cable ya que la fibra, por sí misma, es extraordinariamente frágil.

Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras. Un conexionado correcto de la fibra evita reflexiones de la señal y una mejoría de la calidad de la transmisión.

Investigación

En la voz «fibra óptica» de Wikipedia puedes encontrar información sobre este medio de transmisión, así como de los conectores utilizados en sus instalaciones para redes de ordenadores. Después de leer esta página puedes acudir a la dirección **http://www.lanshack.com/fiber-optic-tutorial.aspx** en donde encontrarás un tutorial sobre la instalación de distintos tipos de fibra óptica. En la página **http://www.conectalo.com/redes-fibra-optica-c-2104_203.html** también puedes encontrar abundante información comercial sobre conectorización de fibra óptica.

Para finalizar este epígrafe es conveniente repasar las características de los cables STP y UTP a modo de comparativa.

a) En cuanto al *throughput* (rendimiento de la transmisión): ambos tipos de cables pueden transmitir desde 10 Mbps hasta 10 Gbps.

b) En cuanto al coste del cable: STP es más caro que UTP.

c) En cuanto al coste de instalación: STP vuelve a ser más caro puesto que requiere la conexión de su malla externa metálica a tierra, algo que no es requerido en UTP. Esta cualidad debe ser tenida en cuenta por el instalador a la hora de hacer el presupuesto de instalación.

d) En cuanto a los conectores: ambos tipos de cableado utilizan conectores RJ45.

e) En cuanto al ruido y la inmunidad a señales no deseadas: STP es mucho más inmune al ruido que UTP, que está escasamente protegido.

1.2. Sistemas de fibra óptica

La fibra óptica permite la transmisión de señales luminosas. La fibra, que suele ser de vidrio u otros materiales plásticos, es insensible a interferencias electromagnéticas externas. La luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente de señal portadora luminosa para la transmisión de datos. Son necesarias fuentes especializadas: fuentes láser y diodos LED.

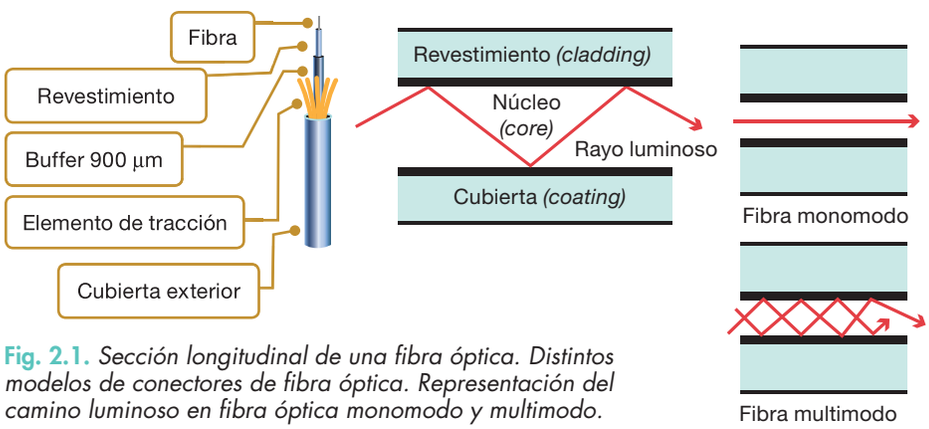


Fig. 2.1. *Sección longitudinal de una fibra óptica. Distintos modelos de conectores de fibra óptica. Representación del camino luminoso en fibra óptica monomodo y multimodo.*

El cable de fibra óptica consta básicamente de un núcleo, un revestimiento y una cubierta externa protectora (Fig. 2.1). El núcleo es el conductor de la señal luminosa. La señal es conducida por el interior de este núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterior como la adición de nuevas señales externas indeseadas.

Actualmente se utilizan dos tipos de fibras ópticas para la transmisión de datos: fibras monomodo y fibras multimodo. Las fibras multimodo pueden ser de índice gradual o de índice escalonado.

a) La fibra **monomodo** (*Single Mode Fiber,* SMF) utiliza un núcleo estrecho (menor de 10 micras de diámetro) que es atravesado por un láser en un único camino, sin apenas reflexiones de la luz en las paredes.

b) La fibra **multimodo** (*Multimode Fiber,* MMF) tiene un diámetro que varía entre las 50 y 115 micras, aunque la más común es la de 62,5 micras, que conduce la luz procedente de múltiples diodos láser cada uno con un ángulo distinto en la entrada de la fibra. En este caso la luz viaja haciendo múltiples reflexiones en las paredes internas de la fibra.

Finalizamos con un resumen de las características de la fibra óptica:

a) En cuanto a su *throughput,* puede llegar a 100 Gbps o más.

b) En cuanto al coste, su instalación es más cara que el cable de cobre. Las interfaces de red también son algo más caras que sus equivalentes para par trenzado.

c) En cuanto al ruido, no es afectada por el ruido ni las emisiones radioeléctricas.

d) En cuanto a la escalabilidad, puede crear segmentos de red desde metros hasta 40 km o más.

1.3. Sistemas inalámbricos

Estos sistemas se utilizan en las redes de área local por la comodidad y flexibilidad que presentan: no son necesarios complejos sistemas de cableado, los puestos de la red se pueden desplazar sin grandes problemas, etc. Sin embargo, su velocidad de transmisión no es muy alta y sus parámetros de transmisión están legislados por las administraciones públicas, que los restringen.

El medio de transmisión en los enlaces de radio es el espacio libre, con o sin atmósfera, a través de ondas electromagnéticas que se propagan a la velocidad de la luz. Para llevar a cabo la transmisión se utiliza un sistema de antenas emisoras y receptoras.

Fig. 2.2. *Dispositivos inalámbricos utilizados en redes de área local: punto de acceso con doble antena (arriba), tarjeta de red inalámbrica con interfaz USB (abajo, a la izquierda) y tarjeta de red PCI con interfaz inalámbrica de una única antena (abajo, a la derecha).*

De modo general, cuanto mayor es la frecuencia de la señal que se emite, tanto más sensible es a algunos problemas, de modo que la distancia máxima entre las antenas emisora y receptora debe ser menor para garantizar una comunicación íntegra.

La propagación por el medio atmosférico produce en ocasiones problemas de transmisión provocados por los agentes meteorológicos. Estos efectos negativos se pueden comprobar fácilmente en las emisiones televisivas cuando las condiciones climáticas no son favorables en forma de interferencias, nieve, rayas, doble imagen, etc.

Los efectos físicos que pueden alterar las comunicaciones inalámbricas son los siguientes:

- **Reflexión:** se produce cuando la onda electromagnética se encuentra con un obstáculo reflectante que hace que la señal se refleje en él y produzca interferencia consigo misma. Suele haber reflexión en las paredes, suelos y techos.
- **Difracción:** en este caso la señal divide su camino, lo que hace que se bordeen los obstáculos que se encuentra y que el destino reciba la misma señal por varios caminos, pero desfasados uno de otro. Son obstáculos que producen difracción las esquinas de paredes, el mobiliario, etc.
- **Dispersión:** es la difusión o reflexión de la señal en múltiples y diferentes direcciones sin un control direccional definido. Suele ocurrir cuando la señal se encuentra con obstáculos cuyas dimensiones son muy pequeñas. Producen dispersión de la señal obstáculos como la lluvia, la niebla o el granizo.

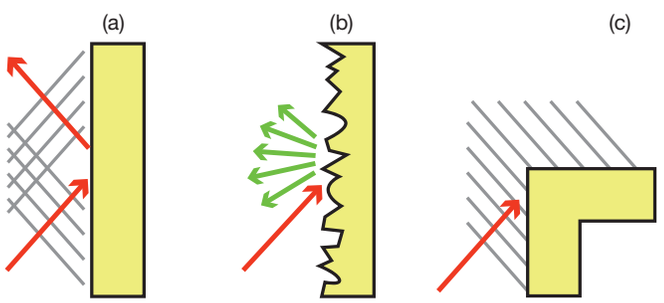


Fig. 2.3. *Efectos de reflexión (a), dispersión (b) y difracción (c).*

En la actualidad se están utilizando masivamente los sistemas inalámbricos en el despliegue de redes de área locales debido a que permiten la movilidad de los equipos y facilita un acceso cómodo a los servicios de red desde lugares en donde es difícil llevar un cable.

CEO

SMR_RL_AAbad_02_RadioterrestresSatelites.docx

Documento que contiene información sobre:

1. Sistemas radioterrestres.
2. Satélites artificiales.

Actividades

1. ¿Cuándo utilizarías cables de pares UTP y cuándo STP? ¿Qué ventajas e inconvenientes tendría sustituir el cable STP por fibra óptica?
2. Enumera algunos elementos positivos y otros negativos de utilizar sistemas inalámbricos para las comunicaciones en redes de ordenadores.
3. Sobre una instalación de red real identifica los tipos de cables utilizados en el sistema de cableado. Utiliza una aplicación gráfica para hacer un croquis sencillo de la instalación de la red, identificando con colores o símbolos los distintos tipos de cables.
4. Describe los factores que generan problemas en la radiación de las señales inalámbricas.

Vocabulario

Conector: también llamado interfaz físico, es un dispositivo que sirve para unir circuitos eléctricos.

2. Dispositivos de conexión de cables

Los cables que forman parte de una red de transmisión de datos no pueden utilizarse si la señal eléctrica no entra en ellos debidamente. De esta función se ocupan los conectores, que no son más que interfaces que adecuan la señal del cable a la interfaz del receptor.

Frecuentemente, los conectores de una misma familia se duplican en forma de «macho» o «hembra», que deben acoplarse mecánicamente en la instalación.

2.1. Conectores para redes

El conector es la interfaz entre el cable y el DTE o el DCE de un sistema de comunicación, o entre dos dispositivos intermedios en cualquier parte de la red. En una LAN, los conectores conectan los cables a las tarjetas de red.

Algunos de estos conectores se describen a continuación (Tabla 2.4):

- **RJ11, RJ12, RJ45.** Estos conectores se suelen utilizar con cables UTP, STP y otros cables de pares. Para estos cables habíamos definido distintas clases y categorías, que son también heredadas por los conectores. Por tanto, al adquirir los conectores se debe especificar la categoría del cable que se pretende utilizar con ellos.
- **AUI, DB15.** Utilizados en la formación de topologías en estrella con cables de pares, o para la conexión de transceptores a las estaciones.
- **BNC.** Se utiliza con cable coaxial fino, típico de Ethernet. Mantiene la estructura coaxial del cable en cada conexión.
- **T coaxial.** Es el modo natural de conectar una estación en un bus de cable coaxial.
- **DB25 y DB9.** Son conectores utilizados para transmisiones serie.

En el caso de redes inalámbricas no podemos hablar de conectores sino de antenas de radiación. En cada extremo de la comunicación debe haber una antena o varias, dependiendo de la tecnología utilizada. Por tanto, las antenas, realizan la función de transceptores puesto que convierten la señal eléctrica de los circuitos electrónicos en ondas de radio.

Investigación

En la página web **http://www.lanshack.com/make-cat5E.aspx** puedes encontrar un tutorial sobre la confección de latiguillos de categoría 5/5e. Después, en el laboratorio, puedes intentar hacer algunos latiguillos de red que posteriormente deberás probar. También puedes ayudarte de las páginas de Wikipedia accesibles desde las voces «RJ11», «RJ45» y «BNC», en donde encontrarás más información tecnológica característica de estos conectores.

Puedes repetir el ejercicio con el cableado de categoría 6. Tienes ayuda en la página **http://www.lanshack.com/make_cat_6_cable.aspx.**

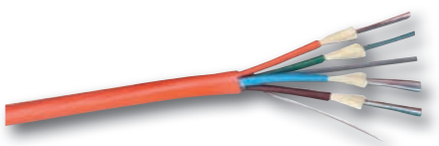
Cable coaxial 	**Cable UTP** 	**Fibra óptica y su protección** 
RJ45 	**DB25** 	**DB9** 
Piezas que componen un conector BNC para cable coaxial y un terminador de 50 W 	**Conectores RJ45** 	**Conectores y latiguillos para fibra óptica** 

Tabla 2.4. *Distintos tipos de cables y conectores.*

Pero cables y conectores no son los únicos elementos físicos de la red. También hay que considerar la conducción de los cables por las instalaciones arquitectónicas, los elementos que adecuan los cables a las tarjetas de red, etc.

- **Balums y transceptores.** Son capaces de adaptar la señal pasándola de coaxial, twinaxial, dual coaxial a UTP o, en general, a cables de pares, sean o no trenzados. La utilización de este tipo de elementos produce pérdidas de señal ya que deben adaptar la impedancia de un tipo de cable al otro.
- **Rack.** Es un armario que recoge de modo ordenado las conexiones de toda o una parte de la red (Fig. 2.4).
- **Latiguillos.** Son cables cortos utilizados para prolongar los cables entrantes o salientes del rack.
- **Canaleta.** Es una estructura metálica o de plástico, adosada al suelo o a la pared, que alberga en su interior todo el cableado de red, de modo que el acceso a cualquier punto esté más organizado y se eviten deterioros indeseados en los cables.
- **Placas de conectores y rosetas.** Son conectores que se insertan en las canaletas, o se adosan a la pared y que sirven de interfaz entre el latiguillo que lleva la señal al nodo y el cable de red.

Fig. 2.4. *Vistas de un rack para cableado estructurado.*

2.2. Conectores para fibra óptica

Los conectores más comunes utilizados en instalaciones de fibra óptica para redes de área local son los conectores ST y SC (Tabla 2.5). En redes FDDI suele utilizarse el conector de tipo MIC.

Otros conectores utilizados son el FC, MT Array y SC Duplex. En la página **http://en.wikipedia.org/wiki/Optical_fiber_connector o en http://www.fiber-optics.info/articles/fiber_optic_connectors** puedes encontrar descripciones y fotografías de estos conectores.

	El **conector SC** *(Straight Connection)* es un conector de inserción directa. Suele utilizarse en conmutadores Ethernet de tipo Gigabit. La conexión de la fibra óptica al conector requiere el pulido de la fibra y la alineación de la fibra con el conector.
	El **conector ST** *(Straight Tip)* es un conector semejante al SC pero requiere un giro del conector para la inserción del mismo, de modo semejante a los conectores coaxiales. Suele utilizarse en instalaciones Ethernet híbridas entre cables de pares y fibra óptica. Como en el caso del conector SC, también se requiere el pulido y la alineación de la fibra.

Tabla 2.5. *Conectores para fibra óptica de tipo SC y ST.*

2.3. Herramientas utilizadas en la conectorización

La creación de las conexiones de la red debe ser realizada con sumo cuidado. La mayor parte de los problemas de las redes de área local, una vez que han entrado en su régimen de explotación, se relacionan directamente con problemas en los cables o en los conectores.

Cuanto mayor sea la velocidad de transmisión de las señales de la red tanto mayor será la necesidad de calidad en los conectores y las conexiones que conforman.

Antes de su utilización, cada cable construido debe ser probado para asegurarse de que cumple con las especificaciones de calidad requeridas en la instalación. Por tanto, si no se tiene seguridad en la construcción del cable con sus conectores incluidos, el cable debe rechazarse.

Claves y consejos

En las instalaciones de fibra óptica hay que tener mucho cuidado con la torsión del cable ya que se trata de un material muy frágil. Los fabricantes de fibra suelen recomendar que la fibra no se doble con radios de curvatura inferiores a 25 veces el diámetro del propio cable de fibra.

Ampliación

Actualmente, y sobre todo en entornos domésticos, se está utilizando el cableado eléctrico de fuerza de la instalación para transmitir señales de radio que se aprovechan para intercomunicar los ordenadores de un domicilio o para asegurarse la conexión a Internet que algunas compañías eléctricas han comenzado a comercializar. A esta tecnología se la conoce con el nombre de PLC (*Power Line Communications,* Comunicaciones mediante cable eléctrico). Obviamente, los ordenadores conectados a una red PLC deben disponer de las interfaces adecuadas que permitan la inserción de señal de comunicaciones por la red eléctrica sin que se vean dañados por la potencia eléctrica de suministro.

Fig. 2.5. *Algunas herramientas para la conectorización de cables de pares.*

Fig. 2.6. *Kits de conectorización de fibra óptica (a la izquierda) y de cables de pares (a la derecha).*

Claves y consejos

Como la mayor parte de las herramientas utilizadas en la conectorización de cables son cortantes o punzantes, debe ponerse especial cuidado en respetar todas las normas de seguridad oportunas para evitar cortes. Es una buena práctica profesional disponer todas las herramientas necesarias correctamente ordenadas sobre la mesa de trabajo antes de practicar un conector. Así mismo, conviene separar los residuos metálicos y electrónicos del resto para su correcto reciclaje, evitando contaminaciones innecesarias del medioambiente.

CEO

SMR_RL_AAbad_02_ConectoresSerie.docx

Documento que contiene información sobre el estándar RS-232 de conexión para cables serie.

Las herramientas utilizadas en la construcción de las conexiones del cableado dependerán del tipo de cable y de conector. Las grandes empresas que diseñan y construyen sistemas de cableados suelen disponer de las herramientas adecuadas para su conectorización. También hay que disponer de la documentación correspondiente al tipo de conector que se va a confeccionar.

Estas herramientas toman formas especializadas como alicates, cuchillas y crimpadores. Se pueden adquirir en los comercios especializados por separado o formando parte de kits para cada tipo de cable.

Además de las herramientas de conectorización, de los cables y de los conectores, son necesarios algunos otros componentes que cooperan en la calidad de la instalación. Nos fijaremos aquí en algunos de modo orientativo:

- **Macarrón termorretráctil.** Se trata de cables huecos construidos con un material plástico termorretráctil, es decir, que se comprimen por aplicación de calor. Suele instalarse en la unión del cable con el conector para que una vez apretado por efecto del calor, el conector quede más sólidamente sujeto al cable.
- **Bridas.** Son elementos plásticos que abrochan los cables entre sí o a los armarios y canaletas por donde se instalan de modo que se fije la trayectoria del cable y se impida su movilidad.
- **Etiquetas identificativas.** Constituyen un sistema de información que se adjunta a cada cable para tenerlo identificado en todo momento.
- **Otro tipo de herramientas** más comunes como tijeras, pelacables, destornilladores, punzones, cuchillas, pinzas, resinas, cinta aislante, etc.

Actividades

5. ¿Cuáles son los conectores más utilizados en las instalaciones de red con fibra óptica? ¿Qué características mecánicas tiene cada uno de ellos? ¿Qué modos de propagación se utilizan para conducir la señal luminosa en el núcleo de una fibra óptica?

6. Enumera los elementos utilizados en la conectorización de cables así como su función.

7. Sobre una instalación de red real identifica los conectores utilizados en el sistema de cableado. Confecciona en una hoja de cálculo una clasificación que permita un sencillo cómputo de los componentes utilizados que sea la base de un futuro inventario. Se puede incluir en este estudio también el sistema telefónico.

3. La tarjeta de red

El adaptador de red, tarjeta de red o NIC (Network Interface Card) es el elemento fundamental en la composición de la parte física de una red de área local. Cada adaptador de red es una interfaz entre el hardware y la red.

El adaptador puede venir o no incorporado con la plataforma hardware básica del sistema. En algunos ordenadores personales hay que añadir una tarjeta separada, independiente del sistema, para realizar la función de adaptador de red. Esta tarjeta se inserta en el bus de comunicaciones del ordenador personal convenientemente configurada. Un equipo puede tener una o más tarjetas de red para permitir distintas configuraciones o poder atacar con el mismo equipo distintas redes.

3.1. Descripción y conexión del adaptador

La conexión de la tarjeta de red al hardware del sistema sobre el que se soporta el host de comunicaciones se realiza a través de la interfaz de conexión. Cada ordenador transfiere internamente la información entre los distintos componentes (CPU, memoria, periféricos) en paralelo a través de un bus interno. Los distintos componentes, especialmente algunos periféricos y las tarjetas, se conectan a este bus a través de unos conectores llamados slots de conexión, que siguen unas especificaciones concretas.

Por tanto, un slot es el conector físico en donde se «pincha» la tarjeta. Es imprescindible que la especificación del slot de conexión coincida con la especificación de la interfaz de la tarjeta.

La velocidad de transmisión del slot, es decir, del bus interno del ordenador, y el número de bits que es capaz de transmitir en paralelo, serán los primeros factores que influirán decisivamente en el rendimiento de la tarjeta en su conexión con el procesador central.

Actualmente las interfaces más usadas en servidores y equipos de sobremesa son PCI (en sus diversas variedades), PCMCIA para ordenadores portátiles y USB tanto para portátiles como para equipos de sobremesa (Fig. 2.7).

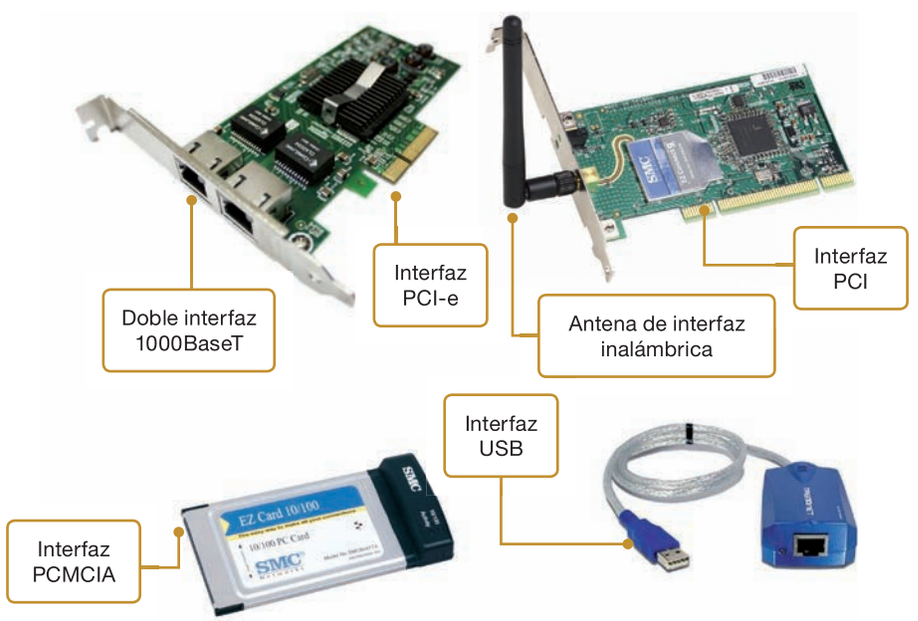


Fig. 2.7. *Adaptadores de red con interfaz PCI-e para cable UTP con doble puerto Ethernet (arriba izquierda), para redes inalámbricas con bus PCI (arriba, derecha), con interfaz PCMCIA para portátiles (abajo, izquierda) y con interfaz USB (abajo, derecha).*

Seguridad

Es preciso guardar unas medidas de seguridad mínimas para garantizar que la electrónica de los componentes no se estropee por una imprudente manipulación, como por ejemplo, descargarse de electricidad estática, trabajar en un ambiente seco y limpio, etc.

Claves y consejos

Es una buena práctica para el administrador de la red visitar con alguna frecuencia la sede web de los fabricantes de las tarjetas de red de la instalación para comprobar que los controladores que tiene instalados con las tarjetas de red coinciden con la última versión que distribuye el fabricante. Normalmente, las nuevas versiones corrigen problemas y hacen mejorar el rendimiento del hardware.

Antes de hacer una actualización de un controlador de tarjeta de red conviene hacer una copia de seguridad del sistema operativo o al menos crear un punto de restauración por si el nuevo controlador diera algún problema.

Ampliación

Este software es un programa de muy bajo nivel denominado **controlador** o *driver* de red que es específico para cada adaptador. Normalmente cada fabricante construye su propio controlador para cada una de las tarjetas que fabrica, aunque los sistemas operativos tienen integrados controladores para las tarjetas más comunes. Si el sistema operativo es avanzado, es posible que estos controladores estén firmados digitalmente con objeto de garantizar su procedencia como signo de estabilidad y correcto funcionamiento.

En el caso de adaptadores para redes inalámbricas el procedimiento de instalación es semejante aunque no utilizaremos cables, que serán sustituidos por las antenas de radiación que las propias interfaces llevan incorporadas.

Como en cualquier otra tarjeta, el adaptador de red necesita de un software **controlador** que conduzca sus operaciones desde el sistema operativo. De este modo, las aplicaciones a través del sistema operativo tienen controlados los accesos al hardware del sistema, y en concreto, a la red.

Sobre este controlador pueden establecerse otros programas de más alto nivel y que tienen funciones específicas relacionadas con los protocolos de la red. A estos programas se les llama ***«packet-drivers»,*** porque son los encargados de la confección de los paquetes o tramas que circularán por la red. Estos paquetes están construidos de acuerdo con las especificaciones de los protocolos de capa superior adecuándolos a las características del medio físico de la red.

Cuando instalamos hardware nuevo en un sistema y lo arrancamos, si este soporta la tecnología *plug & play,* entonces nos avisará del nuevo hardware encontrado y tratará de instalar con nuestro consentimiento, más o menos automáticamente, los controladores apropiados para hacer funcionar correctamente esos nuevos dispositivos.

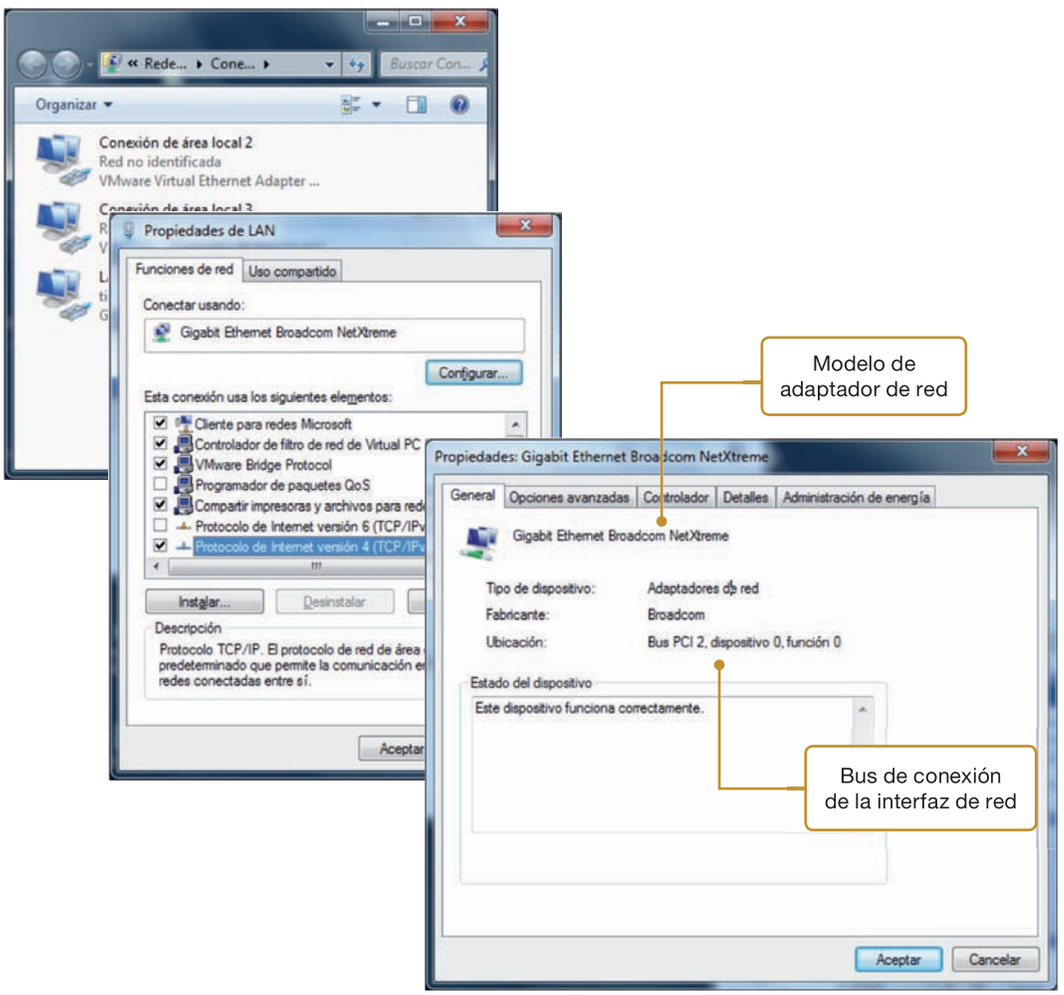


Fig. 2.8. *Configuración del adaptador de red en un sistema Windows.*

Ampliación

Algunas tarjetas de red incorporan un zócalo para la inserción de un chip que contiene una memoria ROM (*Read Only Memory,* Memoria de solo lectura) con un programa de petición del sistema operativo del host a través de la red. De este modo el host puede cargar su sistema operativo a través de la red, por ejemplo a través de un servicio de red denominado BOOTP. La petición del sistema la realiza el cliente nada más iniciarse eléctricamente utilizando la tecnología PXE.

En la última generación de tarjetas, la configuración se realiza automáticamente: elección del tipo de conector, parámetros de comunicación con el sistema, etc., aunque requiere hardware especializado en el host. Esta tecnología de configuración automática se llama *plug & play* (enchufar y funcionar o enchufar y listo), y facilita extraordinariamente el trabajo del instalador, quien ya no tiene que preocuparse de los parámetros de la tarjeta.

En ocasiones, el sistema operativo no reconoce automáticamente la tarjeta de red recién instalada. Esto ocurre sobre todo si la tarjeta es más moderna que el sistema operativo. El fabricante de la tarjeta debe proporcionar con la misma su software controlador para los sistemas operativos más comunes.

3.2. Configuración de las tarjetas de red

No todos los adaptadores de red sirven para todas las redes. Existen tarjetas apropiadas para cada tecnología de red: Ethernet, Token Ring, FDDI, redes inalámbricas, etc.

Algunas tarjetas que sirven para el mismo tipo de red se parametrizan de acuerdo con ciertas especificaciones. Por ejemplo, una tarjeta Ethernet puede estar configurada para transmitir a 10 Mbps o 100 Mbps, si está preparada para ello, dependiendo del tipo de red Ethernet a la que se vaya a conectar. También se puede elegir el tipo de conexión: 10Base2, 10Base5, 10BaseT, 100BaseT, 1000BaseT, etc.

Los adaptadores de red se pueden configurar en modo gráfico mediante el Panel de Control (Windows) o el Administrador de red (Linux), aunque también es común utilizar el intérprete de comandos (Windows) o Shell (Linux). Por ejemplo, es común servirse de las órdenes **ifconfig** (Fig. 2.9, abajo) para configurar tarjetas de red cableadas y de **iwconfig** para las tarjetas de red inalámbricas, aunque esto puede variar dependiendo de la distribución concreta del sistema operativo y de su versión.

CEO

SMR_RL_AAbad_02_TarjetaRed.docx

Documento que contiene información sobre:

1. Tipos de tarjetas de red para servidores y clientes.
2. Parámetros configurables en la tarjeta de red.

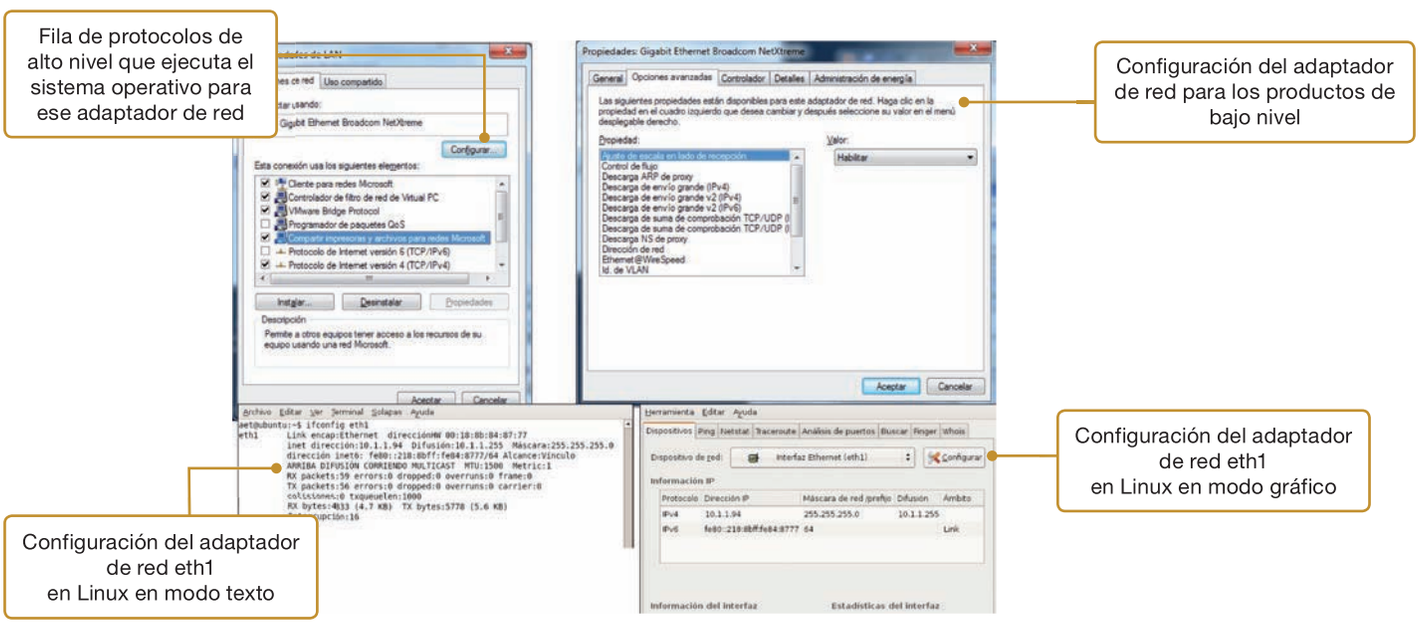


Fig. 2.9. *Arriba, características configurables de un adaptador de red en un sistema Windows. Abajo, ejecución en Linux del comando ifconfig de configuración de una interfaz de red (a la izquierda) y su equivalente gráfico (a la derecha).*

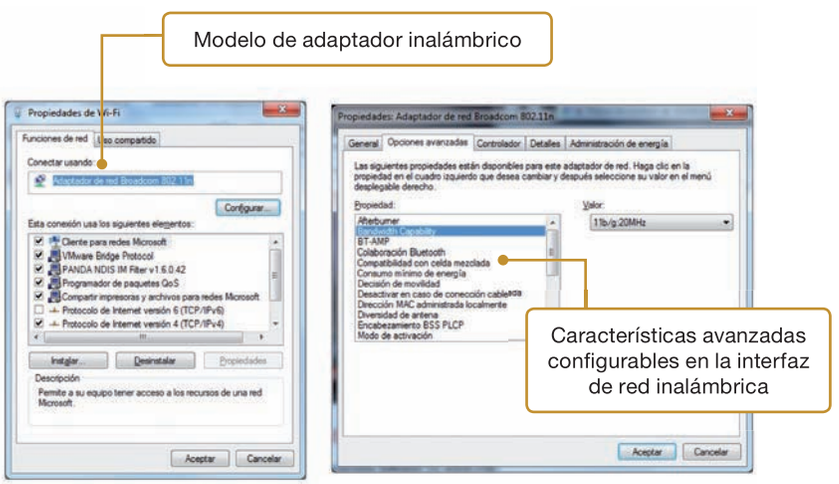


Fig. 2.10. *Configuración de un adaptador de red inalámbrico.*

Investigación

En la página web de Wikipedia seleccionada por la voz «tarjeta de red» puedes encontrar información e ilustraciones de distintos modelos de adaptadores de red. Fíjate bien en ellas y analiza cómo son los buses de conexión tanto hacia el PC en el que se insertan como hacia el cableado de red.

En la página web de Intel tienes información sobre los adaptadores de red que Intel comercializa con todas sus especificaciones técnicas. Puedes empezar tu estudio comparativo de distintos modelos de adaptadores en la página **http://www.intel.com/cd/network/connectivity/emea/spa/desktop_adapters/365264.htm.**

Investigación

En la página **http://www.datacottage.com/nch/eoperation.htm** puedes comprobar mediante una animación cómo se producen las colisiones en Ethernet y cómo se comporta este modelo de red en función del tipo de dispositivo que interconecte los equipos.

En YouTube, también puedes encontrar animaciones y vídeos sobre el funcionamiento de Ethernet buscando: «Ethernet», «CSMA/CD» «Ethernet collisions», etc.

4. Red Ethernet

Ethernet es la red de norma IEEE 802.3, que utiliza el protocolo de acceso al medio CSMA/CD en el que las estaciones están permanentemente a la escucha del canal y, cuando lo encuentran libre de señal, efectúan sus transmisiones. Esto puede llevar a una **colisión** que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio, transmitan una trama de aviso *(jam frame)* y vuelvan a intentarlo. La Fig. 2.11 describe el proceso de contención CSMA/CD.

Si dos nodos en el mismo dominio de colisión se sitúan muy alejados, es posible que no puedan detectar si se produce una colisión y no procederán a la retransmisión de los datos. El problema en la detección se produce porque hay un retardo en la propagación de la señal eléctrica por los cables, que se incrementa con la longitud del cable y con la velocidad de transmisión. Esta es la razón por la que la longitud de los segmentos Ethernet no puede ser tan grande como se desee.

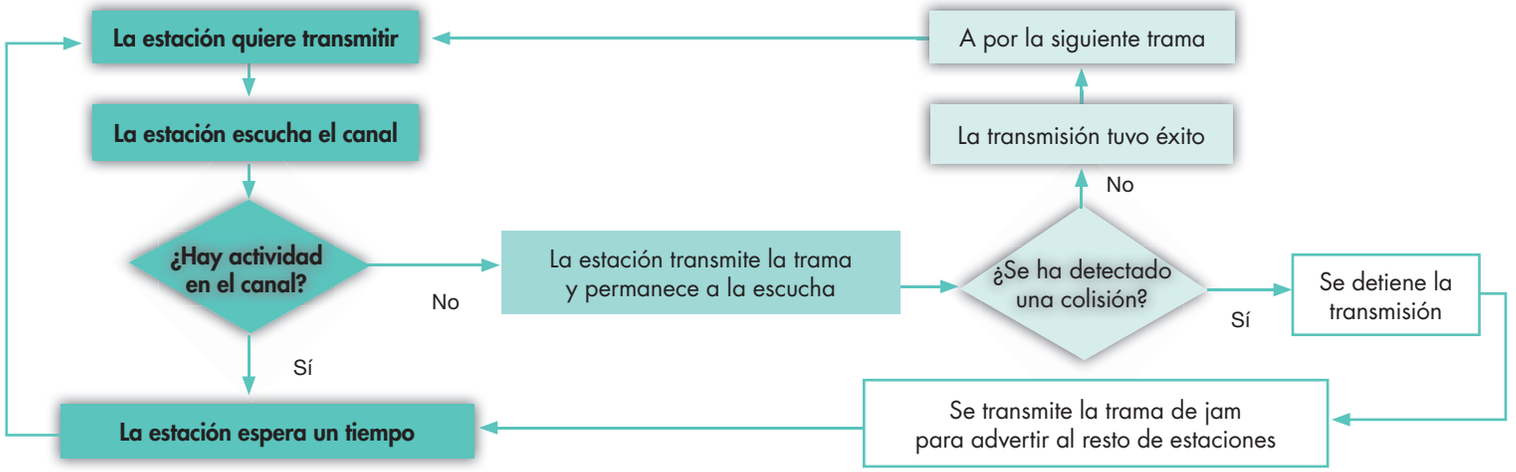


Fig. 2.11. *Diagrama de bloques del proceso de contención CSMA/CD.*

Cualquier estación conectada a una red IEEE 802.3 debe poseer una tarjeta de red que cumpla con este estándar y con los componentes electrónicos y el software adecuado para la generación y recepción de tramas.

La tarjeta o adaptador de red se encarga de verificar las tramas que le llegan desde el canal, así como de ensamblar los datos de información dándoles la forma de una trama, detectar los posibles errores en destino, etc. La tarjeta también es la encargada de negociar los recursos que necesita con el sistema operativo del ordenador en que se instala.

Vocabulario

Una colisión de red se produce cuando las señales procedentes de dos equipos se vuelcan simultáneamente sobre el mismo canal en la misma banda de frecuencia. Un dominio de colisión es la porción de la red en la que dos nodos pueden colisionar.

CEO

S M R _ R L _ A A b a d _ 0 2 _ TramaEthernet.docx

Documento que contiene información sobre el formato de la trama de datos en Ethernet.

4.1. Tipos de Ethernet

El modo en que las tramas IEEE 802.3 son puestas en el medio de transmisión físico depende de las especificaciones de hardware y de los requerimientos del tipo de cableado elegido. Se definen para ello varios subestándares, todos ellos integrados dentro de la IEEE 802.3. Algunos de estos subestándares se describen en la Tabla 2.6.

En algunas instalaciones de alto rendimiento ya se está instalando Ethernet 10G, que sería la red con tecnología Ethernet a 10 Gbps, mayoritariamente sobre fibra, aunque hay algunos intentos con éxito utilizando cableado trenzado de cobre.

- **10GBaseT.** Es un estándar definido en la norma IEEE 802.3an, capaz de transmitir datos a 10 Gbps. Utiliza cableado de categorías 6 o 7 con una longitud máxima por segmento de 100 metros. Suele utilizarse para conectar servidores o estaciones a la LAN, pero no para grandes distancias.
- **10GBaseSR, 10GBaseSW, 10GBaseLR, 10GBaseLW, 10GBaseER y 10GBaseEW.** Son estándares modernos de fibra óptica para transmisiones de 10 Gbps que están definidos en la norma IEEE 802.3ae. Algunas de estas normas pueden llegar a los 40 km.

Ethernet	Medio transmisión	Longitud máx. por segmento	Características
10Base5	Coax 50 W	500 m	Es la especificación original de Ethernet y utiliza coaxial grueso para el transporte de las señales en banda base. También se denomina *Thick Ethernet*.
10Base2	Coax 50 W	185 m	También es una especificación original de Ethernet que utiliza cable coaxial fino, en concreto se suele utilizar el cable RG-58, de 50 ohmios de impedancia, para transmisiones de hasta 10 Mbps. También se denomina *Thin Ethernet*.
10BaseTX	UTP	100 m	Utiliza cables de par trenzado UTP para producir transmisiones de hasta 10 Mbps. Configura la Ethernet como una estrella. Utiliza la regla 5-4-3, que significa que no pueden mediar más de cinco segmentos de red conectados por cuatro repetidores y no más de tres segmentos poblados (que tienen estaciones conectadas). La distancia máxima permitida entre nodos es de 500 metros.
10Broad36	Coax 75 W	1800 m	Transmisiones Ethernet en banda ancha, por tanto, moduladas.
100BaseTX	2 pares STP o UTP categoría 5	100 m	Es semejante al 10BaseT, pero con velocidades hasta 100 Mbps, utilizando cables UTP de categoría 5. Soporta un máximo de tres segmentos interconectados por dos repetidores. Por tanto, la distancia máxima entre nodos es de 300 metros. Está descrito en la norma IEEE 802.3u. Especifica una red de 100 Mbps sobre fibra óptica multimodo. También se considera Fast Ethernet por lo que está definido en el estándar IEEE 802.3u. Utiliza segmentos máximos de 412 metros en semidúplex o de 2000 metros en dúplex. Se permite un único repetidor entre segmentos.
100BaseFX	2 fibras ópticas	500 m	Especifica una red de 100 Mbps sobre fibra óptica multimodo. También se considera Fast Ethernet, por lo que está definido en el estándar IEEE 802.3u. Utiliza segmentos máximos de 412 metros en semidúplex o de 2000 metros en dúplex. Se permite un único repetidor entre segmentos.
100BaseT4	4 pares UTP categoría 3 a 5	100 m	Semejante a 100BaseTX, pero utilizando los cuatro pares.
1000BaseTX	4 pares UTP categoría 5, 5e o 6	100 m	En este caso las comunicaciones siguen la normativa Ethernet pero con velocidades de 1000 Mbps. Sin embargo se necesitan cables superiores al UTP de categoría 5, por ejemplo, el de categoría 5 mejorada (categoría 5e). Además las distancias de cable deben ser mucho más reducidas. Es la base de la tecnología Gigabit Ethernet. El estándar está contenido en la norma IEEE 802.3ab. Puede utilizar únicamente dos segmentos de 100 metros cada uno de longitud máxima, por tanto, la distancia máxima permitida entre nodos es de 200 metros.
1000BaseSX	Fibra multimodo	550 m	Es similar a 1000BaseLX pero compatible con fibra óptica multimodo, por lo que las distancias que alcanza son menores: por debajo de los 500 metros aproximadamente. También permite un único repetidor entre segmentos.
1000BaseLX	Fibra multimodo Fibra monomodo	550 m 2 a 10 km	La velocidad sigue siendo de 1000 Mbps, pero utilizando la fibra óptica como medio de transmisión. Cuando la fibra es multimodo se pueden llegar hasta los 550 m, pero con fibra monomodo se consigue llegar hasta los 2 km y, si la instalación es buena, superar esta distancia hasta llegar a los 10 km. Está definido en el estándar IEEE 802.3z. Se permite un único repetidor entre dos segmentos.

Tabla 2.6. *Tabla de características técnicas de Ethernet a 10, a 100 y a 1000 Mbps.*

4.2. Las colisiones en Ethernet

Cuando Ethernet pone una trama en el bus de la red, esta trama viaja por todo el bus para alcanzar a todas las estaciones que están conectadas a él porque cualquiera de ellas, algunas o todas pueden ser las destinatarias de la información que viaja en la trama.

Sin embargo, una trama no puede saltar a otra red. Se dice que la trama se circunscribe a su dominio de colisión, es decir, una trama solo puede colisionar con otra dentro de su dominio de colisión pues no puede traspasar esta frontera.

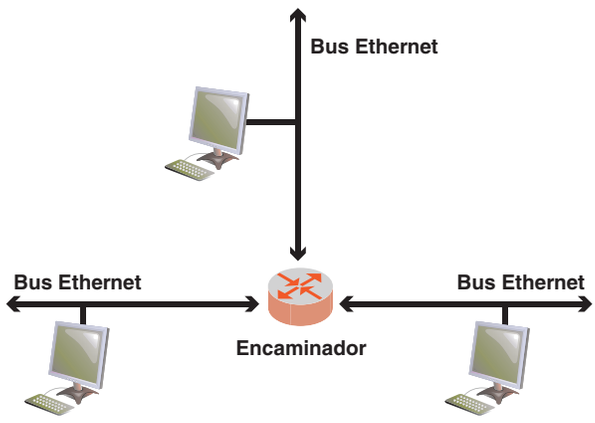


Fig. 2.12. *Tres dominios de colisión definidos por tres buses Ethernet interconectados por un encaminador.*

Truco

Cuando dos redes se van a interconectar mediante un enlace remoto, por ejemplo a través de una línea telefónica, es muy importante que los dominios de colisión de las dos redes queden aislados. Para ello, deberán configurarse los dispositivos de interconexión de las redes de modo que no traspasen las tramas de una red a otra indiscriminadamente. Solo deben pasar las estrictamente indispensables para lograr la funcionalidad de la red, de lo contrario nos encontraremos con una desagradable congestión de red en la línea telefónica.

Investigación

En la página web **http://www.une.edu.ve/~iramirez/telecom2/MediosLAN/Index.htm** puedes encontrar un tutorial de redes locales con una información muy completa sobre cómo se gestionan los dominios de colisión en redes conectadas por repetidores, concentradores y conmutadores. Léete la parte del documento que corresponde a los dominios de colisión para investigar qué dispositivos de red son los más apropiados para evitar al máximo las colisiones.

Actividades

8. ¿Cuál es el nombre técnico del estándar Ethernet? ¿Qué ventajas tiene utilizar PoE para dispositivos de red de bajo consumo?

9. Haz una tabla de los estándares Ethernet más usuales que relacione sus nombres técnicos con algunas de sus características: cableado, velocidad, conectores, etc.

10. ¿Qué es una colisión Ethernet? ¿Y un dominio de colisión?

Cuando un nodo tiene que transmitir información a otro que está en un dominio de colisión distinto necesita acudir a los servicios de otros dispositivos de red intermedios como puentes o enrutadores (Fig. 2.12). Estos dispositivos separan los dominios de colisión y son los encargados de ampliar la red de área local con otros dominios de colisión, cada uno de los cuales se comporta como una red de área local completa. Frecuentemente a estos dominios de colisión se les denomina segmentos de red.

Los protocolos de red que funcionan con direcciones de destino de tipo multidifusión, es decir, con más de un destinatario, pueden producir tormentas de difusión, en donde se generan avalanchas de tramas que pueden colapsar la red. En estos casos es muy importante que los dominios de colisión estén perfectamente acotados. Así, si se produce una tormenta de difusión, quedará confinada a ese segmento de red y el problema no afectará a otros segmentos. Los dispositivos de red de alto nivel incorporan protocolos de gestión y encaminamiento de la multidifusión.

Esto reviste especial importancia si el paso de un segmento a otros se hace a través de una red de baja velocidad: si toda la multidifusión tuviera que pasar por esta red de baja velocidad, todas las comunicaciones quedarían probablemente colapsadas.

4.3. Tecnología Power over Ethernet

Power over Ethernet o abreviadamente PoE es un estándar definido en la noma IEEE 803.af que permite suministrar energía eléctrica a un dispositivo de red a través del cable de datos de la conexión Ethernet. El consumo del dispositivo alimentado debe ser muy reducido, pero puede ser suficiente para alimentar por ejemplo una cámara web, que no necesitaría de una fuente de alimentación alternativa, proporcionándole una mayor independencia y flexibilidad en su instalación.

PoE especifica dos tipos de dispositivos:

a) **PSE *(Power Sourcing Equipment):*** es el dispositivo que suministra la energía, por ejemplo un puerto de un conmutador con tecnología PoE.

b) **PD *(Powered Device):*** es el dispositivo que es alimentado por el PSE, por ejemplo, la cámara web PoE.

La instalación de dispositivos PoE requiere sistemas de cableado de par de cobre con categoría 5 o superior. La corriente eléctrica puede suministrarse por alguno de los pares no utilizados o por alguno de los pares que también lleven datos.

La mayor parte de los conmutadores modernos incorporan PoE, pero en los casos en que no se disponga de esta tecnología es posible incorporar al puerto del conmutador un dispositivo PoE (adaptador PoE) que tiene dos entradas y una salida (Fig. 2.13).

Las dos entradas son una entrada Ethernet (no PoE, que se conecta mediante un latiguillo al puerto del conmutador) y una de corriente. La salida es un conector Ethernet PoE que suministra los datos procedentes del conmutador y además la corriente eléctrica que toma de la fuente de alimentación del adaptador PoE.

Fig. 2.13. *Conmutador PoE (arriba) y adaptador PoE (abajo) para conmutadores no PoE (vista anterior y posterior)*

5. El cableado de red

Fuera del ámbito doméstico, la instalación de un sistema de cableado para una corporación exige la realización de un proyecto en el que han de tenerse en cuenta los recursos disponibles, procedimientos, calendarios de ejecución, costes, documentación, etc.

5.1. El proyecto de instalación

La instalación consiste en la ejecución ordenada, según las directrices del proyecto de instalación de un conjunto de tareas que revierten en proporcionar el servicio que necesitaba el cliente que solicitó la instalación.

Algunas de estas tareas se pueden superponer en el tiempo y habrá que tener esto en cuenta al confeccionar el calendario de instalación. A continuación describimos algunas de estas tareas:

- **Instalación de las tomas de corriente.** Esta tarea suele realizarla un electricista, pero desde el punto de vista del proyecto debemos asegurarnos de que hay suficientes tomas de corriente para alimentar todos los equipos de comunicaciones.
- **Instalación de rosetas y jacks.** Es la instalación de los puntos de red finales desde los que se conectarán los equipos de comunicaciones sirviéndose de latiguillos. La mayor parte de estas conexiones residirán en canaletas o en armarios de cableado.
- **Tendido de los cables.** Se trata de medir la distancia que debe recorrer cada cable y añadirle una longitud prudente que nos permita trabajar cómodamente con él antes de cortarlo. Debemos asegurarnos de que el cable que utilizaremos tenga la certificación necesaria.
- **Conectorización de los cables** en los patch panels y en las rosetas utilizando las herramientas de crimpado apropiadas. A esto se le denomina cross-connect.
- **Probado de los cables instalados.** Cada cable construido y conectorizado debe ser inmediatamente probado para asegurarse de que cumplirá correctamente su función.
- **Etiquetado y documentación del cable y conectores.** Todo cable debe ser etiquetado en ambos extremos, así como los conectores de patch panels y rosetas, de modo que queden identificados unívocamente.
- **Instalación de los adaptadores de red.** Gran parte de los equipos informáticos vienen ya con la tarjeta de red instalada, pero esto no es así necesariamente.
- **Instalación de los dispositivos de red.** Se trata de instalar los concentradores, conmutadores, puentes y encaminadores. Algunos de estos dispositivos deben ser configurados antes de prestar sus servicios.
- **Configuración del software** de red en clientes y servidores de la red.

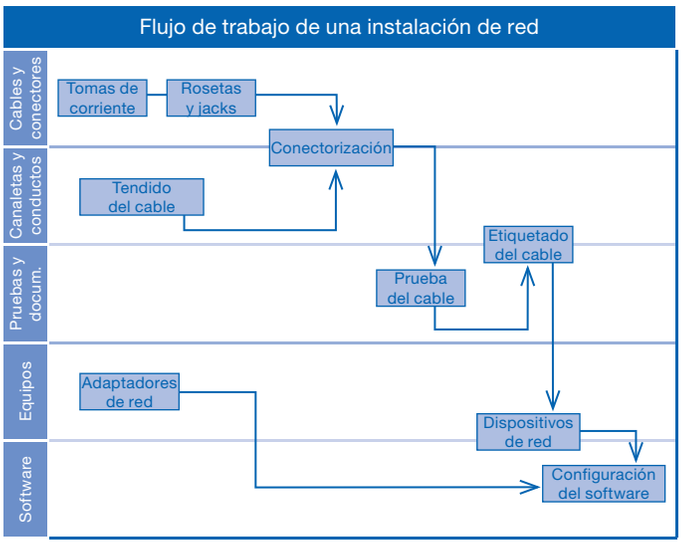


Fig. 2.14. *Flujo de trabajo de los procesos de una instalación de red.*

Claves y consejos

En la realización del proyecto de instalación es muy importante respetar el plazo previsto en cada tarea, sobre todo porque es muy probable que la instalación tenga que coordinarse con la actividad de muchos otros profesionales: electricistas, albañiles, instaladores de aire acondicionado, etc.

Seguridad

Para trabajar con seguridad hay que tener en cuenta las normativas laborales de seguridad en el trabajo. En cuanto a la operación eléctrica ha de cuidarse:

- No trabajar con dispositivos encendidos que estén con la carcasa abierta.
- Utilizar los instrumentos de medida adecuados a las características de las señales con las que se trabaja: no es lo mismo medir los 5 voltios en un componente electrónico que los 220 voltios de fuerza en la red eléctrica.
- Conectar a tierra todos los equipamientos de la red.
- No perforar ni dañar ninguna línea tanto de fuerza como de datos o de voz.
- Localizar todas las líneas eléctricas, así como motores y fuentes de interferencia, antes de comenzar con la instalación de transporte de datos.
- En cuanto a los procedimientos laborales ha de tenerse en cuenta:
  - o Asegurarse bien de las medidas de la longitud de los cables antes de cortarlos.
  - o Utilizar protecciones adecuadas al trabajo que se realiza: gafas protectoras, guantes, etc.
  - o Asegurarse de que no se dañará ninguna infraestructura al realizar perforaciones en paredes, suelos o techos.
  - o Limpieza y, sobre todo, orden.

Vocabulario

Una «U»: es la medida estandarizada de las bandejas de un rack o armario. Es la abreviatura de *Rack Unit*. Equivale a una altura en armario de 1,75 pulgadas (44,45 mm). En cada «U» se incluyen en las paredes del rack tres tornillos de fijación.

Claves y consejos

Al diseñar el tendido de la instalación hay que tener en cuenta que muy probablemente el tendido de red no será el único que deba ir por los falsos suelos o techos y que, por tanto, la instalación de red puede entrar en conflicto con otras instalaciones. Hay que poner especial cuidado en que los cables de datos estén alejados de motores eléctricos, aparatos de aire acondicionado o líneas de fuerza.

5.2. Elementos de la instalación

La instalación de la red no solo se compone de cables y conectores. Estos deben ser fijados a las instalaciones arquitectónicas de los edificios y además hay que hacerlos convivir con instalaciones de otra naturaleza que probablemente ya hayan sido tendidas con anterioridad: agua, fuerza eléctrica, aire acondicionado, etc.

A. Armarios y canaletas

En instalaciones de tipo medio o grande, los equipos de comunicaciones se instalan en armarios especiales que tienen unas dimensiones estandarizadas y en los que es fácil su manipulación y la fijación de los cables que a ellos se conectan. Dentro de estos armarios o racks se instalan bandejas de soporte o *patch panels* para la conexión de jacks o de otro tipo de conectores. La anchura de los racks está normalizada a 19 pulgadas. En la Fig. 2.15 podemos ver un diagrama ejemplo de uno de estos armarios.

La altura de los armarios suele medirse en **«U».** Por ejemplo, el armario de la figura anterior medía 42 «U». Los fabricantes de dispositivos suelen ajustar sus equipos para que se puedan ensamblar en estos armarios ocupando 1, 2 o más «U».

La mayoría de los racks que pueblan los centros de procesos de datos tienen una altura de 42 U (aproximadamente 1,8 metros).

Las canaletas son los conductos a través de los cuales se tienden los cables para que queden recogidos y protegidos convenientemente. Hay canaletas decorativas, de aspecto más acabado cuya misión es ocultar los cables, y canaletas acanaladas que suelen instalarse en los falsos techos o falsos suelos y que son suficientemente grandes como para llevar muchos cables. Las canalizaciones de datos y de fuerza suelen estar separadas para evitar interferencias.

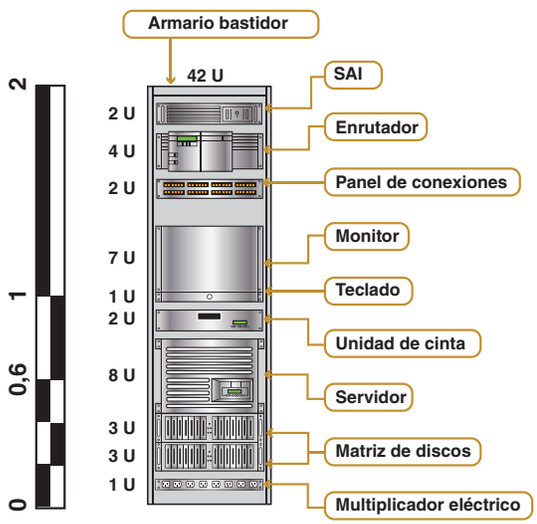


Fig. 2.15. *Esquema de un armario. A la izquierda se ha representado una escala en metros.*

Fig. 2.16. *Diversos modelos de elementos de conexión en armarios y canaletas. A la izquierda y arriba: bandeja de conexiones sobre la que se insertan los módulos de conectorización, que aparecen debajo. A la derecha, roseta de conexiones de múltiples servicios o usuarios, también denominado MUTOA* (Multi-User Telecommunications Outlet Assembly).

B. Suelos y techos técnicos

Las canalizaciones tendidas por suelos y techos técnicos mejoran la limpieza de la instalación haciéndola además mucho más estética.

Existen rosetas especiales para extraer de los falsos suelos tanto datos como fuerza, pero en el diseño hay que poner cuidado para que no estorben al paso y para que queden protegidas con el fin de evitar su deterioro.

Los cables llegan a los armarios a través de los falsos suelos justo por debajo de ellos, lo que ayuda a la limpieza de la instalación. Los distintos cables avanzan ordenadamente, normalmente embridados, por los vértices del armario hasta alcanzar la altura a la que deben ser conectados en algún dispositivo o en algún *patch panel*.

5.3. La instalación eléctrica y de aire acondicionado

Es muy importante que la instalación eléctrica esté muy bien hecha. De no ser así, se corren riesgos importantes, incluso de electrocución. Los problemas eléctricos suelen generar problemas intermitentes muy difíciles de diagnosticar y provocan deterioros importantes en los dispositivos de red.

Todos los dispositivos de red deben estar conectados a enchufes con tierra. Las carcasas de estos dispositivos, los armarios, las canaletas mecánicas, etc., también deben ser **conectados a tierra.**

Toda la instalación debe estar a su vez conectada a la tierra del edificio. Por tanto, habrá que comprobar que el número de picas de tierra que posee es suficiente para lograr una tierra aceptable.

Otro problema importante que hay que resolver viene originado por los cortes de corriente o las subidas y bajadas de tensión. Para ello podemos utilizar sistemas de alimentación ininterrumpida.

Normalmente, los sistemas de alimentación ininterrumpida (SAI) corrigen todas las deficiencias de la corriente eléctrica, es decir, actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etc.

El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que permite guardar los datos que tuvieran abiertos las aplicaciones de los usuarios y cerrar ordenadamente los sistemas operativos. Si además queremos no tener que parar, hay que instalar grupos electrógenos u otros generadores de corriente conectados a nuestra red eléctrica.

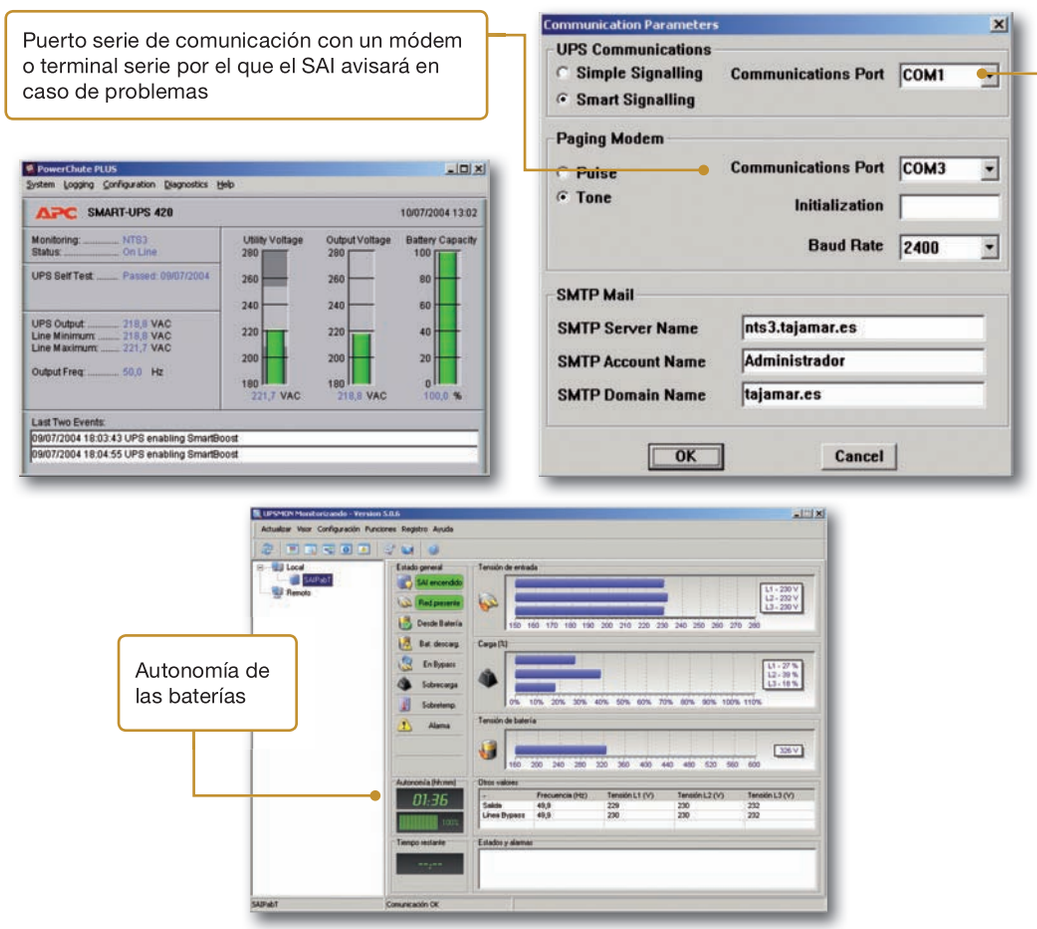


Fig. 2.17. *Parámetros configurables en una estación para el gobierno de un SAI. Arriba, ejemplo de un SAI controlado a través de un puerto serie. Abajo, un SAI que se controla a través de la red de área local.*

Vocabulario

Toma a tierra: en electricidad, es la conexión al nivel de referencia de cero voltios. Las instalaciones de edificios bien construidos incorporan un sistema de cableado subterráneo (picas de tierra) en contacto con el subsuelo del edificio que se toma como el nivel de cero voltios. Todos los dispositivos eléctricos o electrónicos de la instalación del edificio, entre ellos las mallas de los cables STP y las carcasas de los dispositivos de red y racks, deben estar conectados a estas picas de tierra.

Ampliación

La instalación de aire acondicionado debe ser limpia. En los lugares críticos, debe ser redundante, de modo que si alguna consola de aire acondicionado fallara, el resto pueda suplir sus funciones. Además, en caso de rotura de las conducciones o de las consolas, los equipos informáticos no deben verse afectados por flujos de agua.

La temperatura y humedad deben controlarse continuamente y de modo automático mediante termostatos e higrómetros. La mayor parte de los ordenadores actuales incorporan de serie un conjunto de controles internos de temperatura que hacen disparar alarmas en caso de calentamiento de CPU, discos, etc.

Fig. 2.18. *Elementos del cross-connect (arriba), patch panel y latiguillo de conexión (abajo).*

Los servidores pueden comunicarse con un SAI a través de alguno de sus puertos de comunicaciones, de modo que el SAI informa al servidor de las incidencias que observa en la corriente eléctrica. En la Fig. 2.17 se pueden observar algunos de los parámetros que se pueden configurar en un ordenador para el gobierno del SAI. Windows, por ejemplo, lleva ya preconfigurados una lista de SAI de los principales fabricantes con objeto de facilitar lo más posible la utilización de estos útiles dispositivos.

Otra necesidad muy importante en una instalación informática es el control de la temperatura y la humedad del ambiente en que se sitúan los ordenadores y otros dispositivos de red. La regulación de estos parámetros se realiza mediante la instalación de aire acondicionado. Esto reviste una especial importancia en los centros de procesos de datos.

5.4. Elementos de conectividad

Una vez que se tiene tendido el cable en el edificio hay que proceder a realizar las conexiones utilizando conectores, rosetas, latiguillos, etc.

Vocabulario

Cross-connect: operación de interconexión mediante la cual en uno de los lados se sitúan las filas de pines de conexión semejantes a los jacks RJ45, mientras que en el lado opuesto se sitúan las equivalentes filas de conectores. Sobre estos conectores se enchufan los latiguillos que no son más que cables de conexión que actúan de puente entre dos elementos de conexión.

A. *Patch panels* y latiguillos

Un *patch panel* es un dispositivo de interconexión a través del cual los cables instalados se pueden conectar a otros dispositivos de red o a otros *patch panels*.

Sobre un armario se instalan *patch panels* que se conectan al cableado de la instalación por todo el edificio y otros *patch panels* que se conectan a los conectores de los dispositivos de red, por ejemplo a los *hubs* o conmutadores.

Después, una multitud de latiguillos conectarán unos *patch panels* con los otros. De este modo, el cambio de configuración de cableado se realizará cambiando la conectividad del latiguillo sin tener que cambiar nada del cableado largo ni las conexiones a los dispositivos de red.

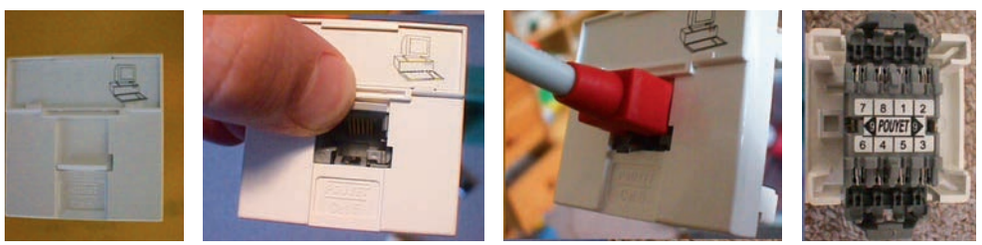


Fig. 2.19. *Elementos que componen una roseta RJ45.*

El cable largo instalado conectará las rosetas con los *patch panels*. Las rosetas *(outlets)* pueden adoptar multitud de formas dependiendo del lugar en que se fijen (canaleta, pared, etc.), del tipo de cable a conectar y del conector que el usuario utilizará. La roseta presenta un conector por un lado y una estructura de fijación de los cables de pares por su reverso, a la que serán crimpados. En la Fig. 2.19 podemos ver los distintos elementos que componen una roseta RJ45.

Truco

Para fijar los filamentos a los contactos debe pelarse la protección del cable para separar cada uno de ellos, que a su vez estarán recubiertos por material plástico. Este material plástico nunca debe quitarse: las cuchillas del contacto perforarán este recubrimiento en el procedimiento de crimpado. La norma especifica que debe descubrirse menos de 1,25 cm de filamentos que deberán destrenzarse.

B. Conexiones a rosetas RJ45

En redes de área local sobre cables UTP deben utilizarse conectores RJ45. De los cuatro pares del cable UTP, la red solo utilizará dos de ellos. Los otros dos pueden utilizarse para telefonía o alguna otra aplicación de telecomunicaciones.

Estos cables se construyen de acuerdo con la norma T568A o la T568B. Los fabricantes de cables UTP los fabrican de acuerdo con un código de colores que tiene que respetarse porque el conector debe crimparse de acuerdo con este código.

Si se observa una roseta por detrás descubriremos que tiene 8 pines o contactos. Algunas incorporan un pin más para la conexión a tierra de la protección del cable (por ejemplo en los cables STP).

Cada filamento de los cuatro pares del UTP debe ir a uno de estos contactos. En la Tabla 2.7 se especifica la relación de pines y colores asociados al filamento.

C. Confección de latiguillos RJ45

Las estaciones de la red se conectan a los dispositivos de red a través de cables construidos con el código de colores y contactos de la tabla anterior en ambos extremos. El cable se confecciona de modo semejante a la conexión a la roseta aunque deberemos cambiar la herramienta que ahora tendrá forma de alicate.

En el conector RJ45 los pines deben leerse con la pestaña del conector hacia abajo, de modo que en esa posición el pin número uno queda a la izquierda.

Sin embargo, cuando se quieren conectar dos ordenadores directamente por sus tarjetas de red sin ningún dispositivo intermedio se tiene que utilizar un cable cruzado, que altera el orden de los pares para que lo que es recepción en un extremo sea emisión en el otro y viceversa. En la Fig. 2.20 se puede ver un ejemplo de construcción de estos dos modelos de cables. En un cable directo, los dos conectores del cable se hacen idénticos, sin embargo en el cable cruzado uno de los extremos se hace como directo y el otro como cruzado.

La asociación de contactos del conector RJ45 con los códigos de colores del cable UTP cruzado sería la expresada en la Tabla 2.8.

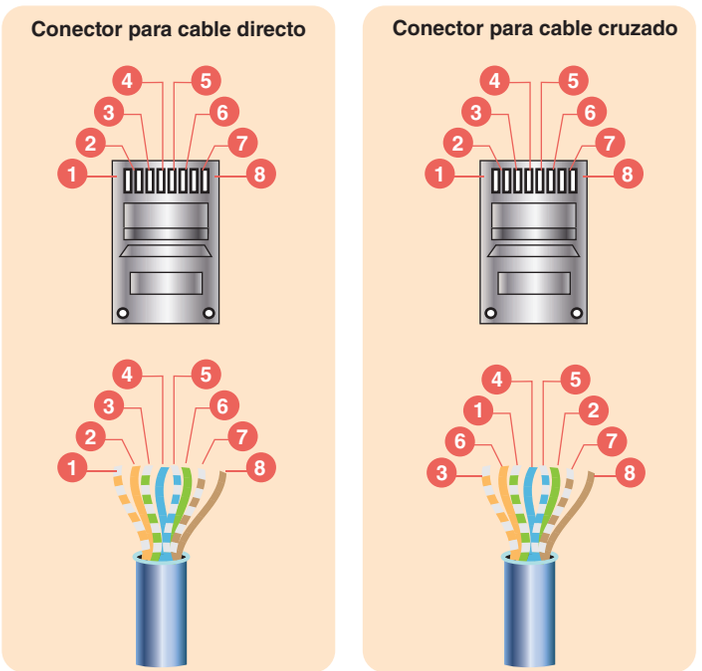


Fig. 2.20. *Cable UTP normal y cruzado.*

Contacto	Color (T568B)
1	Blanco/naranja
2	Naranja
3	Blanco/verde
4	Azul
5	Blanco/azul
6	Verde
7	Blanco/marrón
8	Marrón

Tabla 2.7. *Asociación de pines y colores para el conector RJ45.*

Contacto	Color (T568B)
1	Blanco/verde
2	Verde
3	Blanco/naranja
4	Azul
5	Blanco/azul
6	Naranja
7	Blanco/marrón
8	Marrón

Tabla 2.8. *Asociación de pines y colores para el conector RJ45 en el caso de un cable cruzado.*

Investigación

En la dirección **http://www.gobcan.es/educacion/conocernos_mejor/paginas/montaje.htm** tienes un buen documento gráfico de cómo utilizar los distintos elementos de conexión de un sistema de cableado estructurado. Lee atentamente el documento para que tengas una buena referencia de actuación posterior en el laboratorio.

Laboratorio

Construcción de un cable UTP

La conexión de un ordenador a la red mediante UTP se realiza a través de un latiguillo con dos conectores RJ45. El cable se compone de cuatro pares codificados con ciertos colores. Buscar en Internet el modo de realización del cable y, dotados de las herramientas adecuadas, construirlo. Probar su funcionamiento conectando un nodo a un *hub* utilizando este latiguillo. Se puede conseguir información sobre la construcción del cable en las direcciones siguientes:

- **http://www.coloredhome.com/cable_cruzado/cable_cruzado.htm**
- **http://www.euskalnet.net/shizuka/cat5.htm**
- **http://www.ertyu.org/steven_nikkel/ethernetcables.html**

También se puede probar a buscar la voz «cómo hacer cable UTP» en los buscadores de Internet o en Wikipedia.

Construcción de un cable UTP cruzado

Se trata de construir un cable semejante al del ejercicio anterior pero cruzado. Este cable permite la conexión de dos nodos de la red directamente sin necesidad de un *hub* intermedio. Básicamente su construcción difiere de la del cable UTP normal en que deben cruzarse la recepción de un extremo con la transmisión del otro.

D. Etiquetado de los cables

La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva. Un cable tiene dos terminadores, por tanto cada uno de estos extremos recibirá un nombre.

No es recomendable la utilización de un sistema de etiquetado con relación a un momento concreto, es mejor utilizar nomenclaturas neutras. Por ejemplo, si etiquetamos un PC como «PC de Dirección», y luego el lugar del edificio en donde se ubica la Dirección cambia, tendríamos que cambiar también el etiquetado. Por ello se debe intentar que el etiquetado sea fijo.

Se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector, así sabremos todo sobre el cable: dónde empieza y dónde acaba (Fig. 2.21). Por ejemplo, podríamos etiquetar un cable con el siguiente identificador: **03RS02-05RS24.**

Este cable indicaría que está tendido desde la roseta (RS) número 02 de la sala 03 hasta la roseta 24 de la sala 05.

Las rosetas en las salas 03 y 05 irían etiquetadas con 03RS02 y 05RS24 respectivamente.

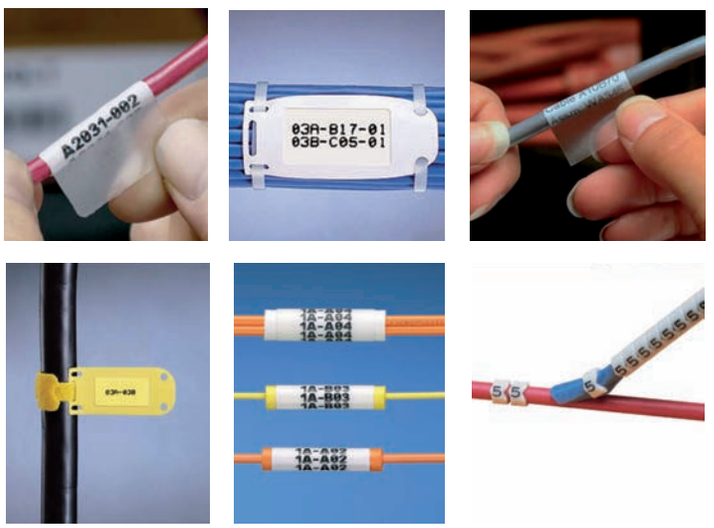


Fig. 2.21. *Algunos modelos de etiquetas para cables.*

Actividades

11. ¿Cuáles son las precauciones básicas que debe tomar el instalador de redes para evitar accidentes laborales?

12. ¿Cuáles son las tareas básicas en un proyecto de instalación de red?

13. ¿Qué es una «U» en un armario de comunicaciones?

14. ¿Cuál es el código de colores para la conectorización de un conector RJ45 según la norma T568B?

15. ¿Cuál es la norma que rige el etiquetado de los cables de comunicaciones en una instalación de red?

16. Utiliza una aplicación de gráficos para construir un croquis aproximado de una hipotética oficina de varias estancias. Elige una de ellas para situar un armario de comunicaciones. En el resto de estancias, diseña una distribución de mesas de trabajo para los oficinistas. Dibuja los cables de conexión de estos puestos con el armario, en donde se situaría un conmutador. Después numera las estancias y etiqueta cada uno de los cables.

6. Cableado estructurado y certificado

Los cambios que se deben realizar en las instalaciones de red, especialmente en su cableado, son frecuentes debido a la evolución de los equipos y a las necesidades de los usuarios de la red. Esto nos lleva a tener en cuenta otro factor importante: la flexibilidad.

6.1. Estructuración del cable

Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: seguridad y flexibilidad. A estos parámetros se le pueden añadir otros, menos exigentes desde el punto de vista del diseño de la red, como son el coste económico, la facilidad de instalación, etc.

La estructuración del cable se consigue construyendo módulos independientes que segmenten la red completa en subsistemas de red, independientes pero integrados, de forma que un subsistema queda limitado por el siguiente subsistema. Estos subsistemas siguen una organización jerarquizada por niveles desde el sistema principal hasta el último de los subsistemas.

Podemos concluir que el cableado estructurado es una técnica que permite cambiar, identificar, mover periféricos o equipos de una red con flexibilidad y sencillez. Según esta definición, una solución de cableado estructurado debe tener dos características: modularidad, que sirve para construir arquitecturas de red de mayor tamaño sin incrementar la complejidad del sistema, y flexibilidad, que permite el crecimiento no traumático de la red.

Vocabulario

Cableado estructurado: es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. La instalación de estos elementos debe respetar los estándares previstos para que un despliegue de cableado se pueda calificar como de cableado estructurado.

CEO

SMR_RL_AAbad_02_Necesidad Cableado Estructurado.docx

Documento que contiene información sobre los factores de conveniencia del cableado estructurado.

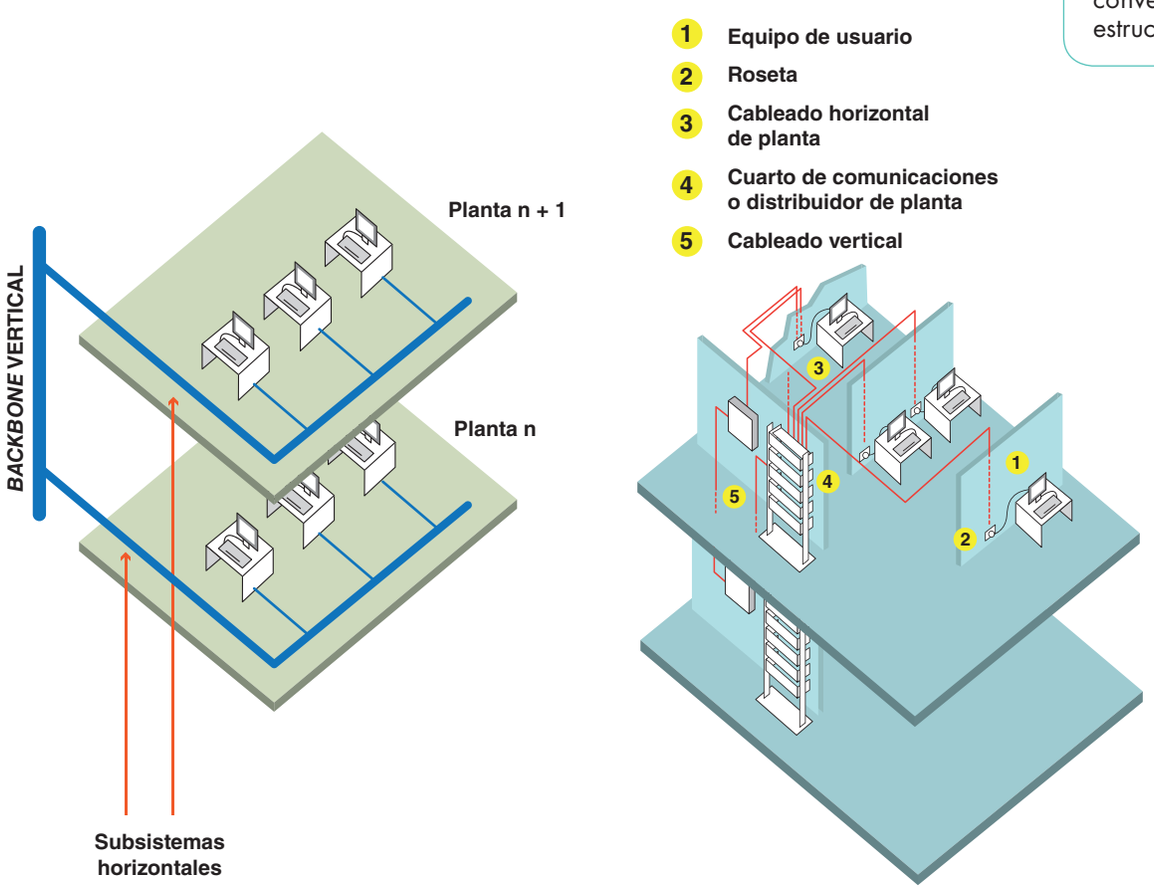


Fig. 2.22. *Cableado estructurado vertical y horizontal en dos plantas de un edificio.*

Partiendo del subsistema de más bajo nivel jerárquico tenemos la siguiente organización:

- **Localización de cada puesto de trabajo.** A cada puesto deben poder llegar todos los posibles medios de transmisión de la señal que requiera cada equipamiento: UTP, STP, fibra óptica, cables para el uso de transceptores y balums, etc.
- **Subsistema horizontal o de planta.** Es recomendable la instalación de una canaleta o un subsuelo por el que llevar los sistemas de cableado a cada puesto. Las exigencias de ancho de banda pueden requerir el uso de dispositivos especiales para conmutar paquetes de red, o concentrar y repartir el cableado en estrella.
- **Subsistema distribuidor o administrador.** Aquí podemos incluir los racks, los distribuidores de red con sus latiguillos, etc.
- **Subsistema vertical o *backbone*.** Este subsistema está encargado de comunicar todos los subsistemas horizontales, por lo que requiere de medios de transmisión de señal con un ancho de banda elevado y de elevada protección.

  Los *backbones* más modernos se construyen con tecnología ATM, redes FDDI o Gigabit Ethernet. Este tipo de comunicaciones es ideal para su uso en instalaciones que requieran de aplicaciones multimedia.
- **Subsistema de campus.** Extiende la red de área local al entorno de varios edificios, por lo tanto, en cuanto a su extensión se parece a una red MAN, pero mantiene toda la funcionalidad de una red de área local. El medio de transmisión utilizado con mayor frecuencia es la fibra óptica con topología de doble anillo.
- **Cuartos de entrada de servicios, telecomunicaciones y equipos.** Son los lugares apropiados para recoger las entradas de los servicios externos a la organización (líneas telefónicas, accesos a Internet, recepción de TV por cable o satélite, etc.), la instalación de la maquinaria de comunicaciones y para los equipamientos informáticos centralizados.

  En algunas organizaciones existen los tres tipos de espacios, en otras el cuarto de equipos incluye al de telecomunicaciones y el de entrada de servicios es sustituido por un armario receptor.

Esta clasificación jerárquica de subsistemas de cableado estructurado no es inflexible. Incluso las denominaciones de cada subsistema pueden variar de unos textos técnicos a otros.

A la hora de diseñar una instalación, lo importante es estructurar los subsistemas para poder documentarlos correctamente y facilitar las ampliaciones o modificaciones de cualquier elemento del cableado.

Claves y consejos

Aunque no es estrictamente indispensable, se recomienda un cuarto de comunicaciones por cada planta.

Investigación

Conéctate a la página **http://platea.pntic.mec.es/~lmarti2/cableado.htm** para ampliar conocimientos sobre las condiciones de instalación de los cuartos de comunicaciones.

En la dirección **http://www.ngsoft.es/cable_estruc.htm** tienes un buen resumen de las tecnologías implicadas en la estructuración del cable.

Ampliación

La especificación de cableado estructurado para cableado UTP exige que los cables no superen los 90 m de longitud, teniendo en cuenta que se pueden añadir 10 m más para los latiguillos inicial y final, de modo que el canal de principio a fin no supere los 100 m, que es la distancia permitida por los cables UTP de categoría 5e. También se especifican, por ejemplo, las distancias que hay que dejar alrededor de los armarios para que se pueda trabajar cómodamente en ellos.

Los estándares más comunes sobre cableado estructurado son en ANSI/TIA/EIA-568 y ANSI/TIA/EIA-569. Los armarios y distribuidores deben cumplir el estándar ANSI/EIA-310.

Laboratorio

Identificación de una instalación de cableado estructurado

En la práctica profesional, frecuentemente hay que actuar sobre instalaciones que ya están en producción. Antes de actuar sobre el cableado hay que tener unos planos de la instalación o, al menos, hacerse cargo de cómo es la instalación actualmente. Para ello hay que identificar los elementos actuales de la red y posicionarlos sobre un croquis.

En la instalación real utilizada en ejercicios anteriores, identificar ahora los elementos que componen el cableado estructurado. Organizar la hoja de cálculo de inventario utilizando como criterio clasificador los diversos subsistemas de cableado estructurado. Seguidamente, sobre un croquis del lugar donde está la instalación de red, trazar las líneas de comunicaciones y adjuntarlo al inventario: este será el inicio de una carpeta de documentación sobre la instalación, que se irá completando con el tiempo.

6.2. Certificación de la instalación

El correcto funcionamiento del sistema de cableado es tan importante que en muchas instalaciones se exige la certificación de cada uno de los cables, es decir, se compara la calidad de cada cable con unos patrones de referencia propuestos por un estándar. En el caso de los cables de cobre, la norma comúnmente utilizada es la ANSI/TIA/EIA-TSB-67 del año 1995, la norma EIA/TIA 568 y su equivalente norma ISO IS11801.

La certificación de una instalación significa que todos los cables que la componen cumplen con esos patrones de referencia y, por tanto, se tiene la garantía de que cumplirán con las exigencias para las que fueron diseñados.

A modo de ejemplo, los parámetros comúnmente probados para los cables UTP de categoría 5 y clase D son el mapa de cableado, la longitud del segmento que no debe superar los 90 metros, la atenuación de la línea y el NEXT *(Near-End Crosstalk)* que proporciona una medida de la autoinducción electromagnética de unas líneas en otras.

Las consideraciones del EIA/TIA 568 especifican los siguientes elementos:

- Requerimientos mínimos para el cableado de telecomunicaciones.
- Topología de la red y distancias máximas recomendadas.
- Parámetros determinantes del rendimiento.

En esta norma se incluyen otras como la TSB36A que determina las características de los cables de pares trenzados de 100 ohmios, la norma TSB40A que indica las características de los conectores RJ45 y sus conexiones, o la norma TSB53 que especifica los cables blindados de 150 ohmios y sus conectores.

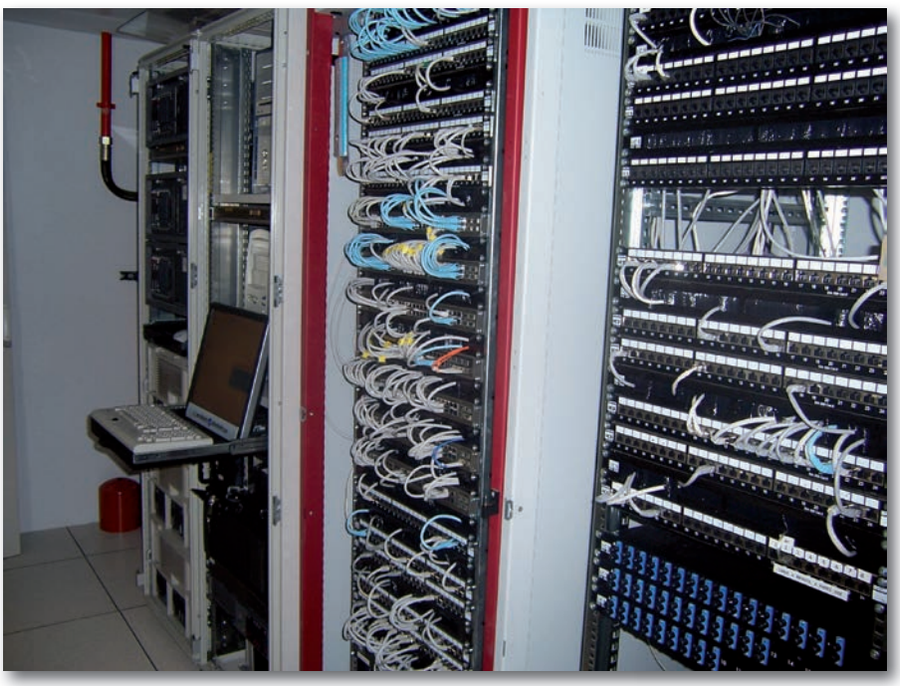


Fig. 2.23. *Vista de un cuarto de comunicaciones instalado con cableado estructurado y certificado.*

Laboratorio

Certificación de cables

Utilizar un dispositivo certificador de cables para comprobar el buen estado de algunos cables. Para ello hay que seguir las indicaciones que el fabricante del dispositivo nos proporcionará en el manual de operación o de usuario. Se sugiere la certificación de la instalación del aula, pero si no es posible se tendrán que confeccionar nuevos cables para su comprobación.

La organización internacional TIA/EIA contempla un conjunto de estándares para el cableado estructurado, que se exponen en la Tabla 2.9.

Estándar	Descripción
TIA/EIA-568-B.1	Estándar con requisitos generales para el cableado de telecomunicaciones en edificios comerciales.
TIA/EIA-568-B.2	Componentes de cableado de par trenzado.
TIA/EIA-568-B.3	Componentes de cableado de fibra óptica.
TIA/EIA-568-B	Estándares de cableado.
TIA/EIA-569-A	Estándares sobre recorridos y espacios de telecomunicaciones para edificios comerciales.
TIA/EIA-570-A	Estándar para el cableado de comunicaciones en zonas residenciales y pequeño comercio.
TIA/EIA-606	Estándar de administración de la infraestructura de telecomunicaciones en edificios comerciales.
TIA/EIA-607	Especificación de requisitos de conexión a tierra.

Tabla 2.9. *Estándares para cableado estructurado de la TIA/EIA.*

A. Dispositivos certificadores

La certificación del cable se realiza con una maquinaria especial que realiza los tests apropiados de manera automática o semiautomática. Existen cuatro tipos de instrumentos para la medición de parámetros de redes que en orden creciente de complejidad son los siguientes: comprobadores de continuidad del cable, verificadores de cables, instrumentos de verificación/certificación y analizadores de redes.

Los fabricantes de estos dispositivos proporcionan en sus manuales los modos de operación correctos para efectuar todas las medidas. Aquí solo mencionaremos algunas generalidades. Los aparatos de medida se componen de dos dispositivos que normalmente se instalan uno al principio del cable (dispositivo activo) y otro al final (dispositivo pasivo) a modo de terminador.

El agente activo envía unas señales muy específicas por el cable a certificar y el pasivo devuelve estas señales para que sean leídas de nuevo por el dispositivo activo. En función de la diferencia entre lo que emitió y lo que ha recibido por los diferentes pares del cable el agente activo averigua los parámetros eléctricos del cable construido. Si se comparan estos valores con los de referencia especificados en las normativas, concluiremos si el cable es o no válido.

Fig. 2.24. *Ejemplos comerciales de instrumentos utilizados en la certificación del cableado. En la parte inferior, gráfico ilustrativo de la medida del parámetro NEXT.*

Actividades

17. Cita los elementos que organizan una instalación construida con cableado estructurado.

18. ¿Qué instrumentos tiene a su disposición el instalador de red para hacer la certificación del cable?

19. Declara como verdaderas o falsas las afirmaciones siguientes:

a) El cableado vertical o de backbone siempre se tiende desde las plantas superiores a las inferiores o viceversa.

b) El subsistema de campus siempre se corresponde con una red MAN.

c) Los latiguillos de red pertenecen al cableado estructurado.

d) Los armarios de comunicaciones no pertenecen al cableado estructurado.

e) Un cable UTP no puede superar los 100 metros de extremos a extremo.

f) La máxima distancia permitida para un cable UTP es de 90 m sin contar los latiguillos de conexión en los extremos.

20. ¿Cuál es el estándar que especifica los componentes de cableado de par trenzado? ¿Y el de fibra óptica?

CEO

SMR_RL_AAbad_02_HerramientasProfesionales.docx

Documento que contiene información sobre los elementos, herramientas y conducciones para el cableado estructurado.

7. Instalación del Centro de Proceso de Datos

Muchas de las instalaciones de diversa naturaleza, no solo de red, pueden realizarse simultáneamente puesto que suelen ser profesionales distintos los que acometen cada parte de la instalación: electricistas, instaladores de cables y certificadores, aire acondicionado, etc.

Una vez que las canalizaciones están instaladas y probadas comienza la instalación de servidores y dispositivos de red. A partir de ese momento se podrán empezar a probar los servicios de red antes de llegar al régimen de explotación.

En el Centro de Proceso de Datos (CPD) es muy importante cuidar la accesibilidad a los equipos de modo que se pueda actuar rápidamente en caso de cualquier avería. Además, las consolas de los servidores tienen que estar bien protegidas ya que quien tiene acceso a una consola podrá manipular fácilmente el servidor al que pertenece. Los lugares en los que se instalan servidores o que contienen puntos neurálgicos de las comunicaciones deben ser lugares de estancia cómoda aunque cerrados bajo llave: frecuentemente el acceso a estos lugares se realiza bajo la supervisión de algún sistema de control de presencia con tarjetas de bandas magnéticas, reconocimiento biométrico u otros sistemas de identificación especialmente seguros.

Fig. 2.25. *Vista de las canalizaciones en la instalación inicial de un centro de proceso de datos.*

El proceso de instalación de un CPD es muy delicado por la gran cantidad de tareas críticas que requiere, por lo que debe diseñarse con sumo cuidado y siempre ayudados de planos y una buena documentación (Fig. 2.26).

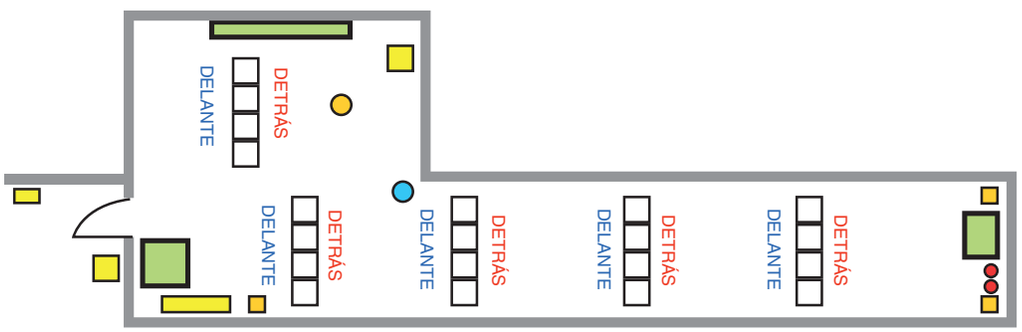


Fig. 2.26. *Plano de instalación de armarios en un CPD.*

Claves y consejos

En el desembalaje de las máquinas es importante guardar en lugar seguro los manuales de usuario, CD de software, garantías de fabricación, información de contacto con el fabricante y cuantos documentos puedan ser útiles en el futuro.

También es prudente guardar algunos embalajes, no todos pero sí alguno de los dispositivos más comunes, porque muchos distribuidores proporcionan su servicio de garantía exigiendo el embalaje original antes de proceder a la sustitución de un equipo averiado.

Claves y consejos

En la manipulación de cajas o elementos pesados conviene poner especial cuidado en derivar el esfuerzo en la flexión de las piernas y no en la columna vertebral o en la torsión del torso. La incorrecta manipulación es una gran fuente de bajas laborales y de lesiones articulares.

Investigación

Frecuentemente las compañías que tienen unos CPD de cierto tamaño duplican los servicios del CPD en un centro de respaldo que se puede contratar con otra compañía. Si ocurre en el CPD una situación de catástrofe, el centro de respaldo atenderá todas las peticiones de los usuarios al conservar una copia de todos los servicios del CPD. Busca las voces «centro de proceso de datos» y «centro de respaldo» en Wikipedia para estudiar las características de estos dos tipos de alojamientos de servidores.

En la página **www.seguridadcpd.com** tienes la web de una compañía que ofrece servicios para los centros de procesos de datos. Fíjate en los servicios y productos que ofrece.

Debido a las necesidades de seguridad crecientes, cada vez se hace más importante un buen diseño del Centro de Proceso de Datos o CPD. Entre los factores que hay que tener en cuenta para este diseño están los siguientes:

- Aire acondicionado redundante.
- Doble acometida eléctrica: si fuera posible, de varias compañías suministradoras distintas.
- Redundancia en las comunicaciones con el exterior: cables de red, fibras ópticas, telefonía, etc. Si es posible, también de diferentes compañías.
- Montacargas, altura y anchura de puertas suficiente para introducir las máquinas que alojará el CPD.
- Seguridad de acceso controlada por puntos de presencia. Vigilancia. Alarmas. Seguridad contra incendios.
- Control de parámetros medioambientales: temperatura y humedad.
- Cuadros de distribución eléctrica independientes y seguros.
- Falsos suelos y techos.
- SAI y generadores de corriente.

Además, como el consumo energético de un CPD es muy elevado, hay que proponer maquinaria de bajo consumo eléctrico que genere menos calor y consiga un doble ahorro económico: menor consumo de energía eléctrica y menor consumo de aire acondicionado. La instalación debe ser muy limpia: el polvo es un enemigo muy importante de los equipos informáticos, que deberán ser limpiados periódicamente como parte de un plan de mantenimiento integral. El acceso a las instalaciones del CPD debe estar restringido a las personas que deban trabajar allí y, además, debe ser controlado automáticamente.

Actividades

21. Declara como verdaderas o falsas las afirmaciones siguientes:

a) El acceso al CPD debe ser siempre restringido.

b) Deben certificarse todos los cables tendidos, pero no los latiguillos de red.

c) El aire acondicionado de un CPD debe ser redundante.

d) Es importante que el CPD se mantenga a una temperatura baja, pero no importa la humedad.

e) Los cables deben llegar al CPD por falso suelo o por falso techo.

f) Los equipos del CPD deben estar protegidos contra subidas de tensión.

22. Diseña una instalación sencilla de cableado estructurado. En primer lugar debes conseguir unos planos reales de una edificación. Sobre estos planos habrá que diseñar una instalación de red para dar servicio a la actividad de una oficina. Esta actividad comprende puestos ofimáticos, algunos servidores, impresoras de red por estancias y conexión a Internet. Se trata de diseñar el sistema de cableado estructurado que dé respuesta a estas actividades utilizando el plano: sitúa el cuarto de comunicaciones, los armarios, el cableado vertical si hay varias plantas, el cableado horizontal, las rosetas de cada puesto de trabajo, etc.

23. Sobre el plano utilizado en el ejercicio anterior se puede seguir trabajando para perfeccionar el diseño. Por ejemplo, de todos los planos conseguidos se puede elegir el que mejor se preste a una instalación más completa. En concreto, céntrate en lo siguiente:

a) Estudia los planos exhaustivamente: muros principales y secundarios, patinillos, galerías, posibilidad de falso suelo o falso techo, etc.

b) Lanza una hipótesis de informatización que mejore la propuesta inicial: qué espacios se van a informatizar y qué servicios se desean cubrir.

c) Realiza una propuesta de cableado estructurado en donde lo más importante será decidir dónde instalar el centro de proceso de datos o el cuarto de instalaciones, que tendrá que tener fácil acceso al exterior y a los sistemas de distribución interior.

d) Realiza el cómputo de materiales necesarios para poder realizar un presupuesto económico de materiales utilizados.

e) Confecciona una carpeta de proyecto.

8. Gestión de residuos

La protección del medioambiente es una misión que corresponde a todos los ciudadanos, pero es una obligación muy especial para un profesional que tiene que trabajar habitualmente con materiales que pueden dañar el entorno medioambiental. Para mitigar el impacto no deseado de la actuación profesional se han habilitado las políticas de tratamiento de residuos.

Estas políticas, que suelen estar expresadas en forma de leyes o de directivas, para el caso de residuos electrónicos o eléctricos tienen como objetivo reducir la cantidad de residuos, la peligrosidad de sus componentes o fomentar la reutilización de los dispositivos de desecho. Para lograr estos objetivos se establecen unas normas que se aplican a la fabricación de los productos o bien a su correcta gestión ambiental cuando se conviertan en residuos.

Hay muchas categorías de RAEE además de los equipos informáticos como son electrodomésticos, aparatos electrónicos de consumo, dispositivos de alumbrado, herramientas, juguetes, aparatos médicos, instrumentos de vigilancia y control o máquinas expendedoras.

Para el caso de equipos de informática y telecomunicaciones se prevé la gestión de los siguientes RAEE:

- Grandes ordenadores. Miniordenadores. Unidades de impresión.
- Ordenadores personales o portátiles (incluyendo unidad central, ratón, pantalla y teclado), tanto en su versión de sobremesa como en sus formatos *notebook* o *notepad*.
- Impresoras, copiadoras, máquinas de escribir eléctricas o electrónicas.
- Calculadoras de mesa o bolsillo.
- Terminales de usuario, fax, télex, teléfonos, contestadores automáticos.
- Aparatos de telecomunicación, transmisión o audio.

La directiva 76/768/CEE de la Unión Europea ordena que los usuarios (consumidores finales) de RAEE utilizados en sus hogares deberán entregarlos, cuando se deshagan de ellos, para que sean gestionados correctamente. La entrega de los RAEE será sin coste alguno para el último poseedor y podrá realizarse en los puntos de recogida previstos en su área geográfica o, siempre que adquiera un aparato que sea equivalente o que realice las mismas funciones que el aparato que desea, en el comercio correspondiente.

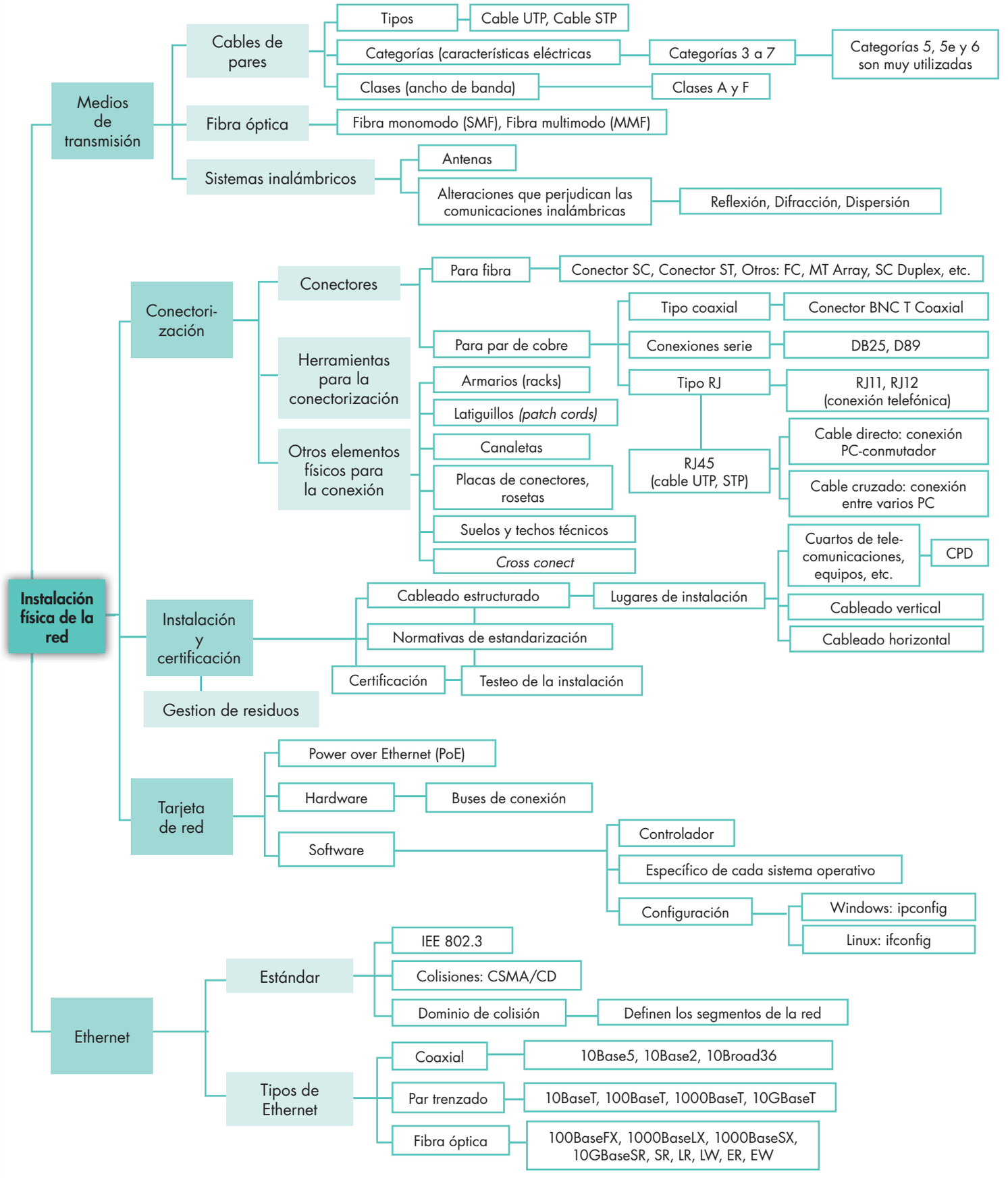
Fig. 2.27. *Punto limpio para recogida de RAEE. Foto J. Albadalejo, archivo del Ayuntamiento de Cartagena.*

Vocabulario

RAEE: siglas de Residuos de Aparatos Eléctricos y Electrónicos. Son los aparatos eléctricos o electrónicos, o sus componentes, al final de su vida útil.

Se considera un aparato eléctrico o electrónico todo aquel que para funcionar necesite corriente eléctrica o campos electromagnéticos, y se utiliza con una tensión nominal no superior a 1000 voltios en corriente alterna y 1500 voltios en corriente continua, además de los aparatos necesarios para generar, transmitir y medir tales corrientes y campos.

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de distintos tipos de cableado (la tercera columna tiene varias posibilidades):

a) UTP	1) Fibra óptica monomodo	i) Inmune a ruidos
b) STP	2) Par trenzado sin apantallar	ii) Categorías y clases
c) SMF	3) Fibra óptica multimodo	iii) RJ45
d) MMF	4) Par trenzado apantallado	iv) SC y ST

2. ¿Qué orden se utiliza para configurar la red en un sistema Linux?

a) ipconfig.

b) ifconfig.

c) netconfig.

d) net ip config.

3. Enlaza los siguientes elementos característicos de distintos tipos de redes (la tercera columna tiene varias posibilidades):

a) 10Base2	1) Fibra multimodo	i) 100 metros
b) 100BaseTX	2) Thin Ethernet	ii)185 metros
c) 1000BaseTX	3) UTP de categoría 5	iii) 550 metros
d) 1000BaseSX	4) 4 pares UTP de categoría 5 o superior	

4. Las colisiones en Ethernet son gestionadas mediante el protocolo:

a) Collision avoidance.

b) CSMA/CA.

c) IEEE 802.1.

d) CSMA/CD.

5. Enlaza los siguientes elementos característicos sobre familias Ethernet:

1. FastEthernet	a. 10 Gbps	i. 10GBaseT
2. GigaEthernet	b. 100 Mbps	ii. 1000BaseT
3. 10GigaEthernet	c. 1000 Mbps	iii. 100BaseT

6. A continuación se citan algunas de las tareas necesarias para hacer una instalación de red, pero están desordenadas. Señálalas en el orden cronológico correcto de ejecución en una instalación real.

a) Diseño de la instalación.

b) Instalación de las tomas de corriente.

c) Etiquetado del cable y conectores.

d) Pruebas y tests de los cables.

e) Conectorización.

f) Configuración de la red en clientes y servidores.

g) Tendido del cableado.

7. Un SAI es un dispositivo electrónico que:

a) Permite la comunicación de los dispositivos de red.

b) Alimenta eléctricamente a los equipos de la red sin cortes de corriente.

c) Cuyas siglas significan Sistema Automático de Interconexión.

d) Convierte la corriente eléctrica alterna en continua.

8. Se desea construir un cable de red UTP cruzado y se hace de acuerdo con el código de colores que aparece representado más abajo para ambos extremos del cable. Se prueba el cable y no funciona. Descubre el error.

Contacto	Primer conector	Segundo conector
1	Blanco/naranja	Verde
2	Naranja	Blanco/verde
3	Blanco/verde	Blanco/naranja
4	Azul	Azul
5	Blanco/azul	Blanco/azul
6	Verde	Naranja
7	Blanco/marrón	Blanco/marrón
8	Marrón	Marrón

9. ¿Qué elemento de los siguientes no pertenece al cableado estructurado?

a) Cableado vertical.

b) Cableado horizontal.

c) Cuarto de comunicaciones.

d) Cuarto de administradores.

10. ¿Qué normativa regula aspectos de la administración del cableado como su etiquetado?

a) EIA/TIA-606.

b) TIA/EIA-568.

c) IEEE 802.5.

d) CPD.

Solución: 1: a-2-(ii y iii), b-4-(i, ii y iii), c-1-(i y iv), d-3-(i y iv). **2:** b. **3:** a-2-ii, b-3-i, c-4-i, d-1-iii. **4:** d. **5:** a-2-iii, b-3-ii, c-1-i. **6:** a, b, g, e, d, c, f. **7:** b. **8:** En el segundo conector deben permutarse los hilos del primer par de modo que no sea Verde/Blanco-Verde sino Blanco/Verde-Verde. **9:** d. **10:** a.

Comprueba tu aprendizaje

I. Identificar los espacios físicos de la red documentándolos con aplicaciones gráficas

1. Analiza si son verdaderas o falsas las siguientes afirmaciones:

   a) Un espacio de red de cableado estructurado es cualquier ubicación en donde llegue un cable de la red.

   b) Los cables de red forman parte del sistema de estructuración del cable.

   c) En cada cuarto de comunicaciones debe haber al menos un conmutador y un encaminador de red.

   d) El CPD siempre es un espacio de red privilegiado del cableado estructurado.

   e) Las canalizaciones de cables siempre han de estar embutidas en tubos.

2. En la dirección web **http://www.novobarra.com.ar/** tienes un amplio catálogo de productos para realizar las conducciones de cables entre los distintos espacios físicos por donde se ha de tender la red así como algún ejemplo de suelo técnico. Realiza un pequeño informe sobre los distintos tipos de canalizaciones que puedes encontrar en el mercado.

II. Desplegar el sistema de cableado de una red local

3. Consigue información sobre las características físicas de los cables UTP y realiza una tabla con los parámetros más significativos. La documentación proporcionada por los fabricantes de los dispositivos certificadores de cables suele ser bastante útil, pero también puedes disponer de mucha información en Internet.

4. Consigue algunos catálogos de cables de fibra óptica de diversos fabricantes y analiza cuáles son los productos comerciales que más se utilizan en la construcción de redes de área local. Fíjate en los precios de fibras semejantes y realiza una tabla comparativa de competencia de precios.

5. En la página web **http://www.une.edu.ve/~iramirez/te1/cableado_estructurado1.htm** tienes una descripción bastante completa de los elementos que intervienen tanto en el subsistema vertical como en el horizontal de un sistema de cableado estructurado. Léelo atentamente y compara el tipo de instalación ideal que refleja el documento con la instalación que utilizas habitualmente. Ahora puedes proponer un conjunto de mejoras para tu instalación.

III. Montar los sistemas de conectorización de la red

6. Recoge una selección lo más exhaustiva posible de conectores utilizados en el cableado de ordenadores u otros sistemas de comunicaciones de aplicación en redes locales. Incorpora una pegatina con el nombre técnico del conector a cada uno de ellos por uno de sus lados. Dale la vuelta a todos los conectores y desordénalos. Ahora tendrás que identificar el nombre específico de cada uno de ellos. Comprueba que la identificación que has realizado es correcta dando de nuevo la vuelta al conector y leyendo la pegatina.

7. Busca algunos proveedores de armarios, canalizaciones y accesorios para confeccionar un catálogo de los productos que serían necesarios para realizar una instalación de red extendida por un edificio. Trata de conseguir también listas de precios.

8. En el contenido de la página web a la que puedes acceder en la dirección **http://sauce.pntic.mec.es/~crer0057/docs/cableado_estructurado/index.html** tienes unas fotografías de una instalación real. Estúdialas con profundidad y elabora un documento similar para la instalación del aula en la que trabajes. Detalla bien el sistema de conectorización.

9. Consigue las herramientas que deben utilizarse para hacer la conectorización y haz un latiguillo con cada tipo de conector. Pruébalo en una instalación de laboratorio para comprobar que está bien hecho. Puedes ayudarte del blog **http://redmaster-cableadoestructurado.blogspot.com/** en donde podrás encontrar imágenes y vídeos de cómo se fabrican.

10. Utiliza un dispositivo certificador de cables para certificar que los cables que has realizado en el ejercicio anterior cumplen con las exigencias técnicas de la norma que hayas utilizado en su confección.

11. Confecciona una tabla con dos columnas. En la primera columna escribe el nombre de los estándares relacionados con el cableado de redes que hayas aprendido hasta el momento. En la segunda columna indica en qué consiste o para qué se utiliza el estándar.

IV. Adquirir buenas prácticas profesionales en instalaciones, seguridad laboral y en el cuidado del medioambiente

12. Conéctate a la página web **http://www.ngsoft.es/index.htm** (o a alguna similar) que corresponde a una empresa que ofrece servicios de instalación, certificación y mantenimiento del cableado. Haz un breve informe con los servicios que ofrece y fíjate especialmente en los precios.

13. Confecciona una hoja de cálculo para realizar presupuestos de canalizaciones en las instalaciones de red. Para ello deberás consultar en Internet listas de precios de los componentes que vayas a utilizar.

    El presupuesto consistirá en describir cuántos componentes hacen falta en la instalación de cada elemento del catálogo para multiplicarlo por su precio unitario

Práctica final

MUY IMPORTANTE:

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

1. Haber comprendido bien los contenidos de las Unidades 1 y 2 que constituyen el primer bloque del libro.
2. Haber leído y comprendido el epígrafe 1 de la Unidad final 9, en donde se describe el proyecto cuyas primeras tareas se resolverán a continuación.

Vamos a hacer aquí la ejecución de la primera fase del proyecto sugerido en la unidad práctica final (Unidad 9). Para ello es imprescindible leer detenidamente el epígrafe 1 de esa unidad.

Los objetivos de esta práctica de bloque 1 son:

- Comprender las fases de diseño de un proyecto.
- Diseñar las canalizaciones de una instalación en función de la arquitectura interior.
- Definir el diseño de una instalación de cableado estructurado.

Después de estudiar las dos primeras unidades de este libro, dispones de todos los conocimientos necesarios para conseguir estos objetivos con la realización de esta práctica. Haremos una resolución por etapas según se sugiere en el epígrafe 1.2 de la Unidad 9.

1. Recogida de documentación y búsqueda de proveedores y profesionales

PHES ha acudido al Ayuntamiento de Torrefría y ha recogido la documentación del concurso público junto con una copia de los planos de la instalación. Con esta información ya se puede poner a trabajar. La primera herramienta de trabajo es la imaginación, puesto que hay que inventarse una solución adecuada que resuelva al más bajo coste posible el problema planteado por el Ayuntamiento.

PHES, que es una PYME, no puede resolver todo el proyecto. Sin embargo, cuenta con la ayuda de proveedores de material y equipos y con otras empresas con las que contrata algunos servicios. El detalle de estos proveedores es el que se describe en la Tabla 1.

Proveedor	Área	Tiempo medio de provisión
Tuboflex	Canalizaciones	1 semana
Elektron	Material eléctrico Instalación eléctrica	2 días
Frigosa	Aire acondiconado	1 mes
Infortec	Equipos informáticos, electrónicos y de comunicaciones	15 días
Telcom	Telefonía e Internet	45 días

Tabla 1. *Lista de proveedores seleccionados para las instalaciones de PHES.*

Los proveedores de PHES han sido seleccionados después de un amplio estudio de mercado para asegurarse de que son de confianza, respetan los plazos de entrega y tienen una buena relación calidad/precio en sus productos. En el caso de los proveedores de servicios como canalizaciones, aire acondicionado o instalación eléctrica también se ha tenido en cuenta que en la ejecución de sus trabajos respetan las normas de seguridad laboral previstas por la legislación vigente.

En el caso de los proveedores de materiales eléctricos y electrónicos se ha comprobado que cumplen la normativa de residuos eléctricos y electrónicos y que además son compañías que poseen una certificación homologada de calidad del tipo ISO 9000. Con esto nos aseguramos de que los proveedores, aun siendo algo más caros que la media —porque cumplir todos estos requisitos cuesta más dinero—, nos proporcionan mayores garantías de eficiencia: el retraso en un pedido puede dar al traste con un proyecto.

En algunos casos, especialmente si la contratación se hace con las Administraciones Públicas (aunque cada vez es más frecuente en otros ámbitos), se exige que las compañías que intervienen en la realización de un proyecto tengan las certificaciones profesionales y de calidad apropiadas para que el contrato sea válido.

2. Presentación de una propuesta técnica

Una vez bien leída y comprendida la publicación del Ayuntamiento, los dos socios de PHES se han reunido para dar a luz un proyecto de resolución en donde se equilibren los aspectos técnicos con los económicos. No se trata de dar una solución eficaz, sino una solución efi-

Práctica final

ciente, es decir, que resuelva el problema planteado pero no a cualquier coste: como cualquier otra empresa, PHES tiene que ser capaz de obtener beneficios con su actividad profesional.

La propuesta que se les ocurre a los dos socios de PHES es la de las Figs. 1 y 2.

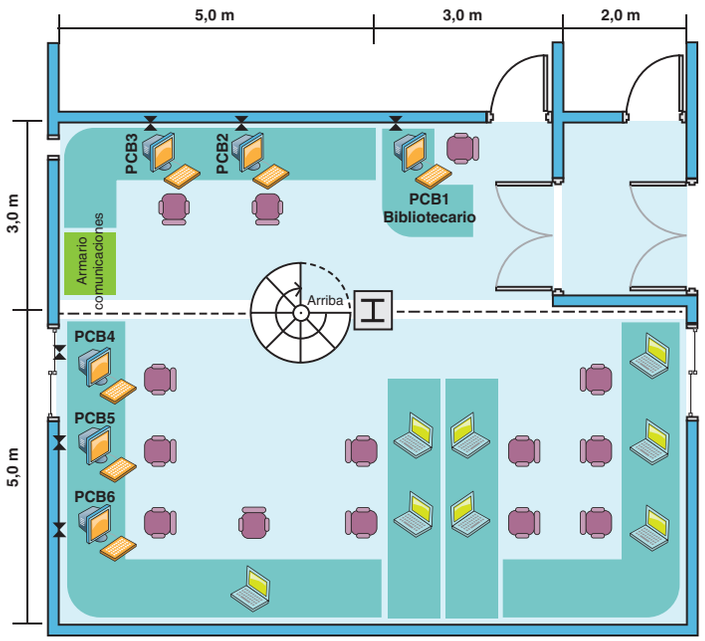


Fig. 1. *Propuesta inicial en planta baja.*

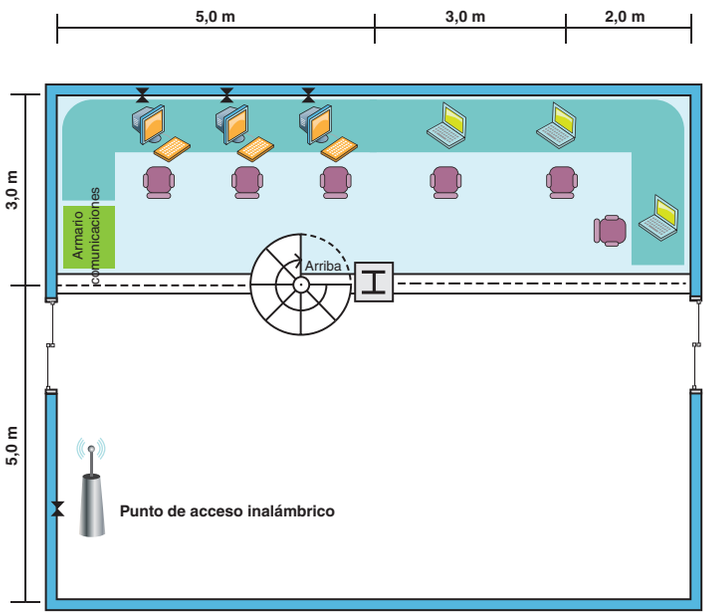


Fig. 2. *Propuesta inicial en planta alta.*

2.1. Hardware

En la propuesta se puede observar el siguiente hardware:

- 5 equipos fijos en planta baja y tres más en planta alta.
- Los portátiles que aparecen en la figura no son de la instalación, representan clientes inalámbricos propiedad de los usuarios de la biblioteca.
- 1 puesto especial para el bibliotecario (en mesa circular, a la entrada).
- 1 punto de acceso inalámbrico para dar soporte a los clientes inalámbricos.
- Dos armarios de comunicaciones para el cableado estructurado (en verde): uno en cada planta.

Los armarios pueden elegirse suficientemente grandes para albergar los equipos servidores que se vayan a utilizar. En principio se proponen dos equipos:

- Un equipo Windows Server para hacer la infraestructura de red básica.
- Un equipo Linux para hacer el proxy/cortafuegos que proporcione un acceso seguro a Internet.

En la pared de la izquierda (en planta baja) se puede observar una abertura en la pared (en la parte superior del plano). Por este orificio es por donde entran los servicios externos al edificio: corriente eléctrica, comunicaciones, etc. Por tanto, ese ángulo del edificio será el candidato para albergar los cuadros eléctricos de entrada y por donde entrará la telefonía e Internet.

Puesto que esa pared es un muro externo, se puede aprovechar ese muro para hacer en él la instalación del aire acondicionado del edificio y, de este modo, asegurarnos de que la temperatura interior es la apropiada para la convivencia humana y la refrigeración de los equipos. La empresa Frigosa se encargará de hacer el cálculo del aire acondicionado necesario y pasará a PHES un presupuesto.

Para la corriente eléctrica se pasará el plano de la propuesta a Elektron para que haga el estudio de los puntos de corriente necesarios y del requisito de cableado de fuerza y la contratación necesaria a la compañía suministradora de electricidad.

2.2. Software y contratación de las comunicaciones

En cuanto al software y las comunicaciones se prevé la siguiente contratación:

Práctica final

Software y comunicaciones	Observaciones
1 Windows Server, con 25 licencias de conexión de cliente.	Cada licencia de cliente puede hacer una conexión al servidor. Software propietario. Este servidor proporcionará los servicios de disco e impresoras.
1 Linux cortafuegos/ proxy.	Distribución IPCOP. Software gratuito.
9 Windows (XP o superior).	Software propietario.
9 licencias antivirus para estación y 1 licencia para servidor.	Dependiendo de la elección del cortafuegos requerirá una licencia más de antivirus o no.
2 pequeños conmutadores (uno para cada planta).	Se colocarán dentro de los armarios de comunicaciones.
1 punto de acceso inalámbrico.	Puesto que la planta alta es solo media planta, el vano permite el paso de la señal inalámbrica sin dificultad entre las dos plantas.
1 conexión ADSL.	Bastaría con una conexión de 10 Mbps.
1 teléfono.	Se puede utilizar la misma línea que el ADSL, pero se situará en el puesto del bibliotecario.

Tabla 2. *Descripción del software necesario y la contratación de comunicaciones.*

2.3. ¿Qué se puede hacer con esta solución de red?

Ahora hay que plantearse qué es lo que venimos a solucionar con este hardware, software y servicios contratados. Tendremos que revisar punto por punto si con esta solución cumplimos los requisitos de la oferta pública demandada por el Ayuntamiento y observamos que efectivamente los cumplimos. En la Tabla 3 podemos concretar algunos de estos servicios:

Caso	Observaciones
Un usuario de la biblioteca se presenta en un equipo fijo para navegar por Internet.	Puede hacerlo, hay equipos fijos y se ha contratado un acceso de banda ancha.
Un usuario lleva su propio portátil a la biblioteca y desea navegar o consultar los fondos.	Puede hacerlo. Hay una instalación inalámbrica y puntos de corriente por toda la instalación.
Un usuario no sabe cómo configurar en su equipo el acceso a Internet.	La documentación y entrenamiento final del proyecto indica cómo configurar los equipos de los usuarios para que tengan acceso a los distintos servicios.
¿Pueden varios usuarios acceder a Internet simultáneamente?	Sí. Se va a configurar un servidor proxy para compartir el acceso a Internet.
¿El acceso a Internet es seguro?	Se instalará un cortafuegos asociado al proxy para asegurar la red.
Los usuarios quieren consultar los fondos y archivos de la biblioteca.	Podrán consultarlos a través de los servicios de carpetas compartidas con esa documentación.

Tabla 3. *Ensayo hipotético de la funcionalidad de algunos servicios de red.*

3. Análisis de fortalezas y debilidades: ¿qué pasa si...?

Una vez que PHES ha estudiado una solución viable y que cumple con las expectativas el proyecto solicitado, se tiene que plantear mejoras al proyecto que, sin encarecerlo sustancialmente, le proporcionen más ventajas competitivas. No tenemos que olvidar dos ideas:

- El documento que contiene la oferta pública del Ayuntamiento de Torrefría nunca podrá ser completo. Será un resumen, frecuentemente realizado por no expertos, de lo que necesitan.
- PHES tendrá que competir con otras posibles ofertas y, si quiere ganar el concurso, deberá proporcionar la mejor relación calidad-servicios/precio dentro del presupuesto con que se dota al proyecto.

Por eso, una vez llegados a este punto, es razonable hacerse preguntas de mejora del estilo: ¿Qué pasaría si...?

3.1. Mejoras en el hardware

¿Se puede imprimir? El documento de oferta no especifica este servicio, pero parece razonable que en una biblioteca, que es un lugar en donde se manejan documentos, se pueda imprimir. Decidimos incorporar tres impresoras:

- Una impresora para el puesto de bibliotecario (ImpreB1). En esa impresora se podrán hacer los carnés de socio o imprimir peticiones de tipo facsímil de los documentos protegidos de los fondos bibliográficos históricos. Se elige para esta impresora un modelo conectable en red para que pueda ser móvil por toda la instalación.
- Una impresora para la planta baja (ImpreB2). Decidimos que esta impresora, para abaratar costes, se conecte directamente por un cable USB o paralelo al servidor Windows, que irá dentro del armario de comunicaciones de la planta baja.
- Una impresora de red para la planta alta (ImpreA1).

Práctica final

3.2. Mejoras en el software

La mayor parte de los usuarios están entrenados en sistemas Windows, pero con el auge de Linux es posible que acudan usuarios entrenados solo en Linux. ¿Podría un usuario entrenado en Linux acceder sin dificultad a los servicios de red de la biblioteca? Probablemente no. Para solucionar esto, decidimos que algunos equipos clientes corran Windows y otros corran Linux. Con esto, además, nos ahorraremos el coste de algunas licencias de Windows XP o superior.

- En planta baja, los dos equipos cercanos al puesto de bibliotecario correrán Linux, el resto Windows.
- En planta alta, el equipo más lejano al armario también correrá Linux, los otros dos correrán Windows.

Los equipos portátiles propiedad de los usuarios podrán correr cualquier sistema operativo compatible con TCP/IP, que será la red que vayamos a instalar.

3.3 Mejoras en las comunicaciones

Como el número de clientes en la red no es muy elevado, no parece que vaya a haber cuellos de botella en la red de área local. Si necesitáramos mejoras en el acceso a Internet, se podría contratar un acceso ADSL de mayor velocidad, pero esto no modificaría la instalación de la red de área local por lo que no parece relevante en este momento.

Sí cabe preguntarse por la seguridad de los accesos.

- ¿Podemos limitar el acceso a páginas inconvenientes? Tendríamos que contratar ADSL con un proveedor que suministre un servicio de filtrado de páginas o contratar uno para cada PC. Si contratamos uno para cada PC, los clientes inalámbricos (portátiles) no estarán protegidos puesto que al ser propiedad de sus propietarios no tendremos capacidad de asegurar un servicio sobre el que no tenemos autoridad. Por tanto, incluso se podrían cometer delitos desde nuestra instalación sin nosotros advertirlo. Como Telcom proporciona un servicio de filtrado de páginas, decidimos contratar con Telcom un servicio de acceso ADSL filtrado para todas las conexiones.
- ¿Podemos evitar los intrusos en nuestra red desde Internet? De esto se encargará el cortafuegos que instalemos. Decidimos que estará configurado para negar cualquier conexión desde el exterior, puesto que el Ayuntamiento no ha solicitado que haya acceso desde el exterior.

3.4. Otras mejoras

Como la distribución de la biblioteca se debe hacer en dos plantas distintas, nos podemos plantear la instalación de una videocámara cerca del punto de acceso de modo que el bibliotecario pueda vigilar la planta superior y la zona de la inferior, oculta por la escalera de caracol de subida a la planta superior. Esta videocámara puede ir volcando sus imágenes a una carpeta compartida en el servidor para su almacenaje. Además, esta videocámara servirá como elemento activo de videovigilancia en los momentos en que la biblioteca esté cerrada al público.

¿Podría el bibliotecario ver por la videocámara en tiempo real? Sí, si elegimos una videocámara que pueda ser accedida directamente desde el puesto del bibliotecario, por ejemplo, a través de su navegador de Internet. Decidimos que la videocámara tenga tecnología de red TCP/IP y que incorpore un servidor web (Webcam) para que se pueda ver imagen en directo desde un navegador de Internet.

4. Ajuste de la propuesta

Una vez incorporados los nuevos datos, que hacen más competitiva en cuanto a servicios nuestra propuesta, tenemos que hacer un ajuste a la propuesta inicial. Ahora los planos de instalación quedarían así:

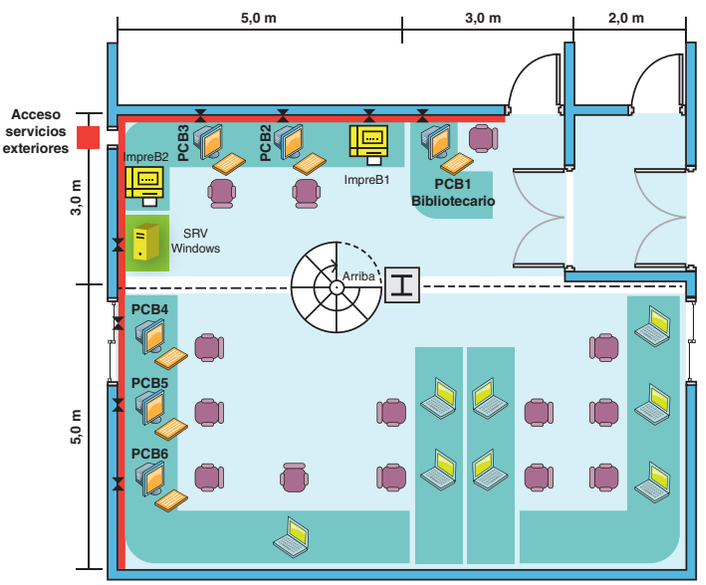


Fig. 3. *Propuesta final para planta baja.*

Práctica final

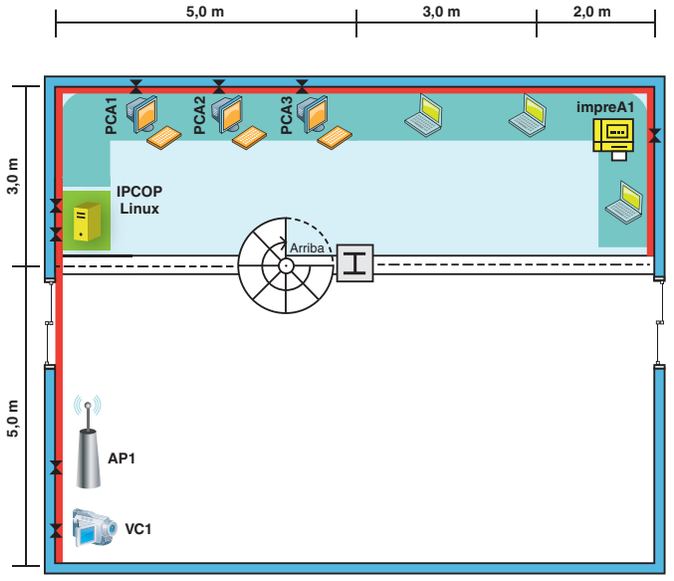


Fig. 4. *Propuesta final para planta alta.*

En las Figs. 3, 4 y 5 se han marcado en rojo las canalizaciones necesarias para el transporte de cables. Las canaletas se instalarán a un metro de altura del suelo, lo que parece suficiente para que sea cómodo conectar los latiguillos de red y los cables de alimentación de los equipos, salvando la altura de las mesas. También se han especificado los nombres de los diferentes dispositivos de red.

En la canaleta irán insertadas las rosetas de red del cableado estructurado y los puntos de corriente que tendrá que instalarnos Elektron. Se le ha pedido que instale cuatro enchufes por cada puesto de trabajo en el caso de los PC fijos y dos enchufes en el caso de los portátiles. Los puestos de impresoras u otros elementos de red llevarán solo una roseta con dos enchufes. Los servidores y el resto de elementos dentro de los armarios no necesitarán alimentación en canaleta puesto que el armario irá electrificado y tomarán la corriente eléctrica de él. Se elegirán rosetas de fuerza dobles (con dos enchufes) integradas en canaletas.

Tendremos los siguientes elementos de fuerza:

Elemento por alimentar	Número de rosetas dobles	Observaciones
Portátiles	8 en planta baja. 3 en planta alta.	Dos enchufes (una roseta de fuerza) por puesto.
PC fijos	6x2 en planta baja. 3x2 en planta alta.	Cuatro enchufes (dos rosetas de fuerza) por puesto.
Impresoras	2 en planta baja. 1 en planta alta.	Dos enchufes (una roseta de fuerza) por impresora.
Otros elementos	1 videocámara. 1 punto de acceso.	Dos enchufes (una roseta de fuerza) por elemento.
Total rosetas de fuerza dobles	34	Cada roseta lleva dos enchufes.

Tabla 4. *Descripción y cómputo de los elementos de fuerza en la instalación.*

En la planta alta, la canalización también se hace a la altura de las mesas como en la planta inferior, sin embargo en el ramal que accede al punto de acceso y a la videocámara, debe instalarse un pequeño segmento vertical hacia arriba (un metro por encima de la canaleta horizontal) para que la videocámara sea capaz de ver lo que ocurre en la planta superior. Según podemos ver en la Fig. 5, instalando la videocámara un metro por encima de la canaleta horizontal (o a dos metros de altura con respecto del suelo de la planta alta) se protege la videocámara de accesos físicos y solo tenemos un ángulo de sombra por debajo de 20°.

Con este plano tenemos que ser capaces de resolver el número de rosetas necesarias y el número de metros de cable para después, al ponerle precio, poder realizar el presupuesto de costes.

Dentro de los armarios de comunicaciones Elektron tiene que instalar una bandeja de enchufes para alimentar los dispositivos electrónicos que se alojen en su interior y algunas otras bandejas en donde alojar los servidores y el encaminador ADSL.

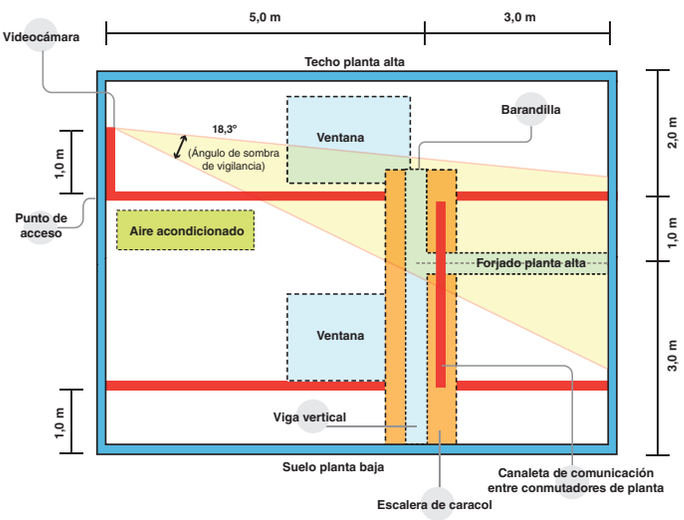


Fig. 5. *Plano de alzado (vertical) de las canalizaciones, visto desde la fachada de entrada.*

Práctica final

4.1 Topología de la red

Es el momento de elegir la topología de la red. Decidimos hacer una red Ethernet con puntos de al menos 100 Mbps, con una estructuración en dos *switches* conectados por un segmento de red vertical (entre armarios en planta baja y alta) de 1 Gbps y hacer una estrella en cada planta. Todos los puntos de red de cada planta tendrán su cable tendido hacia el *switch* de planta.

Los cables tendidos por las canalizaciones seguirán el esquema de las Figs. 3, 4 y 5. Cada cliente se conecta a la roseta mediante un latiguillo de 1 m de longitud que requiere dos conectores RJ45, aunque estos latiguillos se suelen comprar ya hechos y comprobados. El mismo latiguillo servirá para conectar los elementos del *patch pannel* a los puertos del *switch*, uno por cada conexión de red.

Los elementos del *cross connect* conectarán el interior de la roseta de usuario dentro de la canaleta al *patch pannel* dentro del armario de comunicaciones. Cada uno de estos cables tiene su propia longitud en función de la distancia entre el armario que contiene el *patch pannel* y la localización de la roseta dentro de la canaleta. Cada uno de estos cables consume una roseta y un conector RJ45 hembra del *patch pannel*.

Los servidores, situados dentro de los armarios, no requerirán conexiones *cross-connect* y se conectarán directamente a los conmutadores.

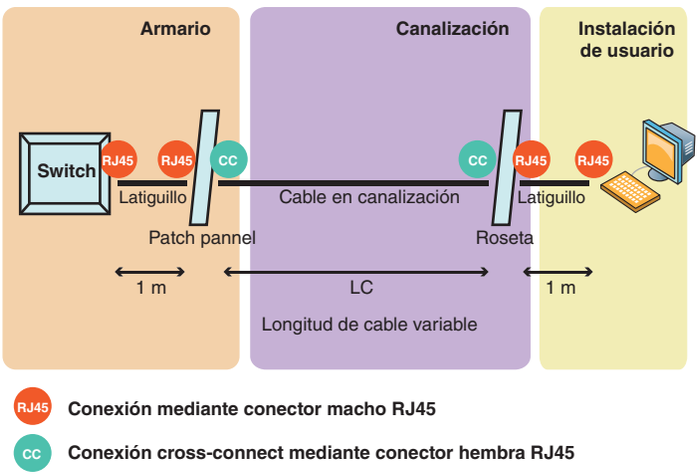


Fig. 6. *Esquema de conexión de un cable de red.*

Ya estamos en disposición de hacer un cálculo aproximado del número de conectores que utilizaremos y del número de metros de cable de red.

Elemento	RJ45	Rosetas	m de cable (LC)	Latiguillos	Función
PCA1	0	1	8	2	Cliente Windows
PCA2	0	1	7	2	Cliente Windows
PCA3	0	1	6	2	Cliente Linux
IPCOP	0	0	0	2	Cortafuegos Linux
ImpreA1	0	1	14	2	Impresora de red
AP1	0	1	5	2	Punto de acceso Wi-Fi
VC1	0	1	6	2	Videocámara
PCB1	0	1	8	2	Cliente Windows
PCB2	0	1	7	2	Cliente Linux
PCB3	0	1	6	2	Cliente Linux
PCB4	0	1	2	2	Cliente Windows
PCB5	0	1	3	2	Cliente Windows
PCB6	0	1	4	2	Cliente Windows
ImpreB1	0	1	8	2	Impresora de red
ImpreB2	0	0	0	0	Impresora local
SRV	0	0	0	1	Servidor Windows
Router ADSL	0	0	0	1	Acceso a Internet
Conexión entre conmutadores	2	0	3	0	Construir un backbone de red
Totales	**2**	**13**	**87**	**30**	

Tabla 5. *Descripción y cómputo de los elementos de cross-connect.*

Práctica final

En IPCOP se han dejado dos latiguillos porque deberá tener dos redes: una interna (la red de área local, LAN) y otra externa (Internet, WAN). Sin embargo, como el servidor cortafuegos estará en el armario no necesitará roseta de red en canaleta.

Suponemos que VC1 es una videocámara IP o webcam.

ImpreB2 no necesita ningún conector de red puesto que se conectará directamente al servidor SRV (Windows) que está dentro del armario. Esto limita que la impresora debe estar tan cerca del armario como le permita el cable USB o paralelo.

SRV, que está dentro de un armario, no necesita roseta y solo un latiguillo para conectar la única red que tiene directamente al conmutador de ese armario.

En el router ADSL, que también se instala dentro del armario, se ha previsto un latiguillo, aunque normalmente viene incluido con el pack del router.

Aunque en la tabla se ha mantenido la columna RJ45, se han puesto los valores a 0 porque se decidió adquirir todos los latiguillos fabricados. Si se decidiera hacerlos en vez de comprarlos, por cada latiguillo añadiríamos 2 conectores RJ45 y un metro más de cable.

No obstante, la conexión entre enrutadores, como requiere un latiguillo muy largo y a medida, se ha decido fabricarlo con al menos 3 metros de cable y dos conectores RJ45.

5. Mapa de profesionales

¿Qué profesionales deben intervenir en la instalación y en qué orden? Han ido apareciendo ya en la descripción del proyecto. Ahora solo hay que poner orden en su actuación.

Suponiendo que ya se haya acabado la obra de albañilería, en primer lugar tienen que entrar los instaladores de aire acondicionado porque tendrán que perforar en los muros exteriores y hacer las canalizaciones de los tubos de aire acondicionado. También tendrán que fijar las consolas de aire a las paredes.

Las tomas eléctricas de los aparatos de aire acondicionado tienen que estar disponibles antes de la conexión de las consolas de aire, pero aquí supondremos que es una instalación eléctrica distinta y separada de la instalación de fuerza para los equipos informáticos.

Al mismo tiempo que los instaladores del aire acondicionado pueden entrar los instaladores de canalizaciones, que tendrán que ponerse de acuerdo con los electricistas que las usarán para los tendidos de cable de fuerza. Normalmente los electricistas harán también los tendidos de cables de red y telefónicos. Si los electricistas son especialistas podrán confeccionar las rosetas.

Los armarios de comunicaciones deberán estar instalados antes de que finalice la actuación de los electricistas ya que estos deberán electrificar los armarios.

Una vez realizadas todas las conexiones del cableado estructurado (salvo los latiguillos) deberán entrar los albañiles y pintores para realizar los remates de rozas y pintura y dejar las paredes limpias.

Seguidamente PHES deberá instalar en su ubicación final todos los equipos. Este será el momento de instalar los latiguillos de red, tanto en los ordenadores de usuario como en los servidores y dentro de los armarios para conectar *patch-pannels* con los puertos de los conmutadores.

También deberá estar ya disponible la conexión ADSL. Solo entonces, podrán comenzar las pruebas de funcionamiento.

6. Elaboración de un presupuesto

Se trata de hacer un recuento preciso del material necesario, conseguir una lista de precios competitivos y calcular el coste final del proyecto.

PHES, que se ha puesto en contacto previamente con sus proveedores, ha conseguido los precios unitarios que se especifican en la Tabla 6.

Práctica final

Área	Concepto	Precio unitario (€)	Cant.	Coste (€, IVA inc.)	Observaciones
Cableado, canalizaciones y elementos en canaleta					
	1 metro cable UTP	0,50	125	72,50	Se presupuestan algunos metros más de los necesarios
	1 conector RJ45	0,25	2	0,58	Para latiguillo entre conmutadores de planta
	1 latiguillo de red	4,00	35	162,40	Se dejarán algunos latiguillos de repuesto
	1 patch pannel 24 conexiones	150,00	2	348,00	Un patch-pannel por cada armario
	1 armario 12 U	450,00	2	1.044,00	Un armario por cada planta
	1 bandeja armario	50,00	3	174,00	Una por cada servidor y otra para encaminador
	1 roseta de red para canaleta	30,00	13	452,40	Tantas como puestos de usuario y periféricos de red
	1 elemento de fueza con dos enchufes en canaleta	30,00	34	1.183,20	
	1 metro canaleta	35,00	38	1.542,80	16 en planta baja, 19 en planta alta y 3 entre plantas
	1 bandeja electrificación de armario	90,00	2	208,80	Una por cada armario
	1 cable USB de 2 metros	6,00	1	6,96	Para la impresora local
Electrónica de red					
	1 conmutador Ethernet 24 puertos UTP 1Gbps	300,00	2	696,00	Uno en cada armario
	1 encaminador ADSL	0,00	1	0,00	Acceso ADSL para toda la instalación (incluye el router gratuito)
	1 punto de acceso inalámbrico	120,00	1	139,20	Acceso inalámbrico para toda la instalación
	1 videocámara IP	250,00	1	290,00	Videovigilancia
	1 teléfono	20,00	1	23,20	Puesto bibliotecario
Equipos informáticos					
	1 estación de red con monitor	400,00	9	4.176,00	8 estaciones de usuario más 1 estación de bibliotecario
	1 servidor más discos de almacenamiento	1.200,00	1	1.392,00	Servidor Windows en armario de planta baja
	1 servidor para cortafuegos	400,00	1	464,00	Basta un hardware semejante a una estación
	1 impresora de red	300,00	2	696,00	Una en planta alta y otra en puesto de bibliotecario
	1 impresora local	220,00	1	255,20	Cerca del armario en planta baja
Software					
	1 licencia antivirus para estación (1 año)	45,00	9	469,80	
	1 licencia antivirus para servidor (1 año, 25 usuarios)	200,00	1	232,00	

Tabla 6. *Presupuesto de ejecución del proyecto (1.ª parte).*

Práctica final

Área	Concepto	Precio unitario (€)	Cant.	Coste (€, IVA inc.)	Observaciones
	1 licencia Windows 7 Pro	180,00	6	1.252,80	
	1 licencia Linux	0,00	3	0,00	
	1 licencia Windows Server para 25 clientes (2008 R2)	650,00	1	754,00	
	1 licencia cortafuegos GNU (IPCOP)	0,00	1	0,00	
Contratación servicios y profesionales (subcontratas)					
	Alta ADSL y línea telefónica			150,00	Oferta del proveedor, que incluye el router
	Instalación aire acondicionado			5.000,00	
	Instalación eléctrica y canaletas			1.500,00	Incluye cables y cuadros eléctricos, conexiones red y certificación
Totales en materiales y contrataciones de servicios:				**22.685,84**	**(IVA incluido)**
Horas de trabajo					
	Gestiones de opción a concurso	100,00	10	1.160,00	Documentación de concurso, confección y presentación de la solución
	Gestión comercial con proveedores	80,00	3	278,40	
	Instalación de equipos cliente	80,00	20	1.856,00	Aproximadamente 2 horas por cada equipo
	Instalación de servidores	150,00	10	1.740,00	6 horas para el servidor Windows y 4 horas para el cortafuegos
	Configuración global de la red	100,00	3	348,00	Configuración router y pruebas de funcionamiento
	Elaboración de la documentación	80,00	4	371,20	
	Entrenamiento y formación	80,00	4	371,20	
Totales en horas de trabajo:				**6.124,80**	**(IVA incluido)**
Costes totales:				**28.810,64**	**(IVA incluido)**

Tabla 6. *Presupuesto de ejecución del proyecto (1.ª parte).*

Como se puede apreciar en la tabla, el coste total del proyecto está por debajo de lo especificado por la oferta pública de contratación del Ayuntamiento de Torrefría, por tanto, en principio es una solución válida para el proyecto.

Hay que notar que el hardware del servidor Windows conviene que sea de 64 bits para poder ejecutar las versiones de sistema operativo de 64 bits. Por ejemplo, si elegimos la versión R2 de Windows Server 2008, no tendríamos más remedio puesto que esta versión de sistema operativo solo puede instalarse sobre 64 bits. Este tipo de restricciones deberán ser tenidas en cuenta si no queremos llevarnos sorpresas desagradables, por ello hay que conocer muy bien los productos que se adquieren y que son compatibles entre sí.

7. Elaboración de un calendario

Teniendo en cuenta los plazos que los proveedores necesitan para suministrar el material y que los profesionales subcontratados consumirán en la ejecución de sus tareas, una propuesta de calendario podría ser la siguiente:

Práctica final

- Solicitar el 1 de abril (fecha de la adjudicación) los servicios de telefonía que son los que más tardan (45 días).
- El 15 de abril contrataríamos el aire acondicionado (que tarda 30 días).
- Quince días después (el 30 de abril) pediríamos los equipos informáticos y electrónicos, que tardarán 15 días en llegar.

El resto de los proveedores no impone unas fuertes restricciones sobre el calendario ya que sus plazos de respuesta son de pocos días.

Supuestos estos hitos en las contrataciones, la actividad profesional específica de PHES podría comenzar el 15 de mayo, según la Fig. 7.

El proyecto se comenzaría a gestionar el 1 de abril, la operación empezaría el 18 de mayo y estaría finalizado el 8 de junio, por lo que estamos dentro de los plazos previstos por la adjudicación de proyecto, que nos daba tres meses. Nosotros hemos consumido dos meses y ocho días. La Biblioteca estará en funcionamiento el día 9 de junio, justo para el inicio de la época estival.

8. Confección del proyecto y presentación a concurso

Una vez elaborados todos estos documentos que hemos estudiado, deben presentarse a concurso la descripción del proyecto y el calendario de ejecución.

El presupuesto no debe presentarse ya que es una adjudicación con una inversión fija. Sin embargo, si el concurso compitiera por la oferta más económica, deberíamos presentar el precio final de presupuesto, lo que nos obligaría a buscar nuevas mejoras presupuestarias para incrementar las posibilidades de adjudicación.

PHES presenta la documentación requerida en la Secretaría del Ayuntamiento de Torrefría unos días antes del final de plazo permitido. En el Ayuntamiento aceptan la documentación, la registran oficialmente y, una vez cumplido el plazo de presentación, una comisión de técnicos administrativos evalúa los proyectos.

Unos días después, PHES recibe la comunicación oficial del Ayuntamiento de que su proyecto ha sido elegido para ser ejecutado. PHES decide esperar al 1 de abril, como tenía previsto, para iniciar las gestiones iniciales de contratación.

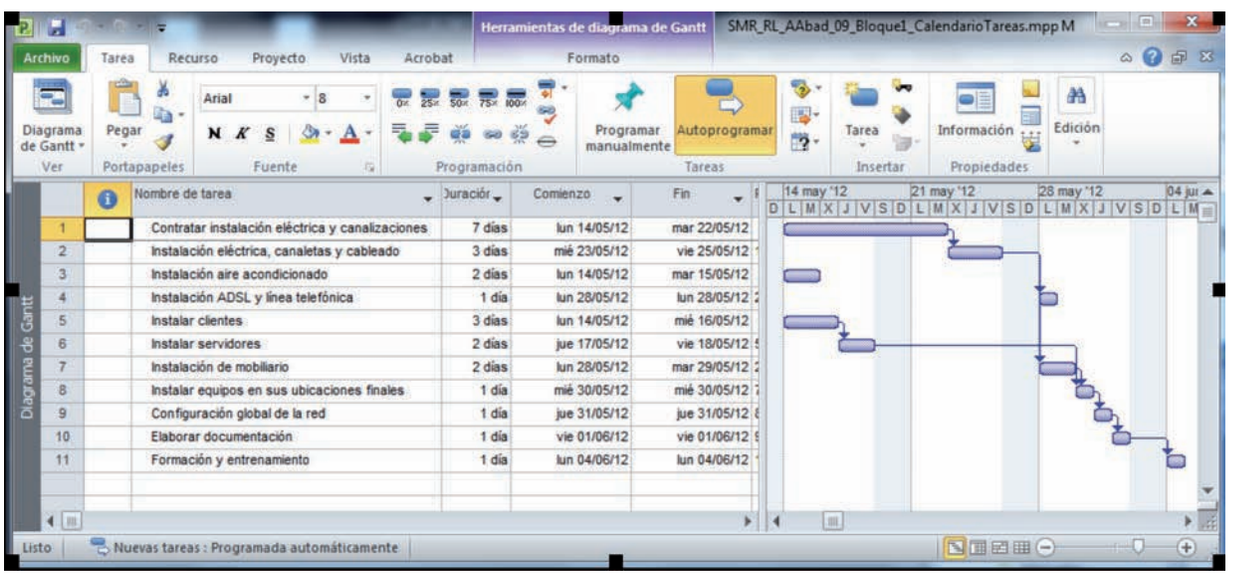


Fig. 7. *Diagrama de Gantt de la ejecución del proyecto.*

Unidad 3

Instalación y configuración de los equipos de red

En esta unidad aprenderemos a:

- Identificar los protocolos y servicios de red proporcionados por los sistemas operativos.
- Utilizar las herramientas básicas para la gestión de protocolos de red.
- Configurar el sistema de direccionamiento de los equipos de la red.

Y estudiaremos:

- Los sistemas operativos disponibles para la red.
- Los componentes de las pilas de protocolos estandarizados.
- Las órdenes de ejecución asociadas a las utilidades de la red.

Ampliación

Microsoft tiene sistemas operativos cliente y servidor. Cada uno de ellos se comercializa con distintas versiones: domésticas, profesionales, empresariales, etc. Las más actuales son Windows 7 en su versión cliente y Windows Server 2008 R2 para la versión servidor, aunque ya están anunciadas las versiones Windows 8, tanto para cliente como para servidor.

1. El sistema operativo de red

Gran parte de la funcionalidad de la red depende del software que se ejecuta en cada uno de sus nodos. Este software se sustenta sobre el sistema operativo y, a su vez, este lo hace en el hardware. De este modo, la red se integra totalmente en el sistema y se hace difícil distinguir lo que es propio de la red de lo que es más específico del sistema operativo. Para ello, los sistemas de red se apoyan en los protocolos, que también serán desarrollados en esta unidad.

El sistema operativo de cualquier sistema conectado a la red es muy importante porque debe interactuar con otros sistemas de la misma o de otra red. Por ejemplo, debe soportar aplicaciones que «hablan» en red, tiene que brindar servicios a otros equipos o servirse de los que otros le proporcionan y, además, tiene que ser interoperable.

1.1. Sistemas operativos comerciales

Los fabricantes de sistemas operativos comercializan versiones distintas en función de que vayan a actuar como servidores o como clientes. La máxima interoperabilidad se produce entre sistemas del mismo fabricante, pero la interoperabilidad ha crecido sobre todo porque actualmente todos los sistemas operativos hablan TCP/IP.

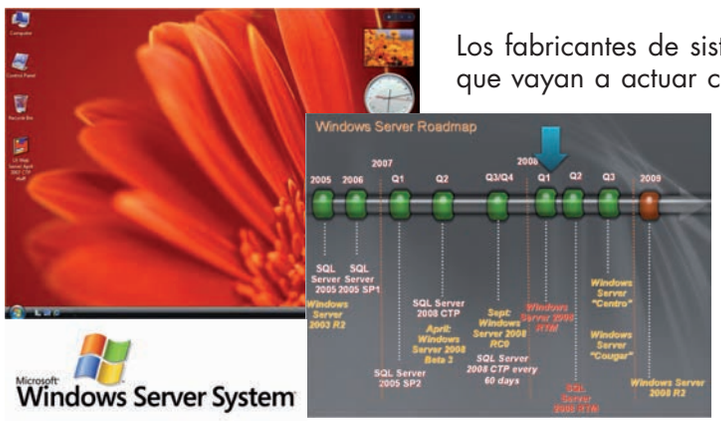


Fig. 3.1. *Logotipo de una gama de productos de servidor de Microsoft y ejemplo de escritorio de Windows Server 2008 R2 (izquierda). A la derecha, calendario de lanzamientos* (roadmap) *utilizado para la presentación de productos de Microsoft.*

A. Microsoft Windows

Windows es el nombre genérico de los sistemas operativos de Microsoft. Aunque tradicionalmente NetBeui ha sido el protocolo de red nativo de los sistemas de Microsoft accesible a través de NetBIOS, actualmente el protocolo nativo adoptado por Microsoft es TCP/IP. Sobre él se ha seguido conservando la interfaz NetBIOS por compatibilidad con las aplicaciones de red anteriores.

Microsoft tiene varias gamas de sistemas operativos que van desde los sistemas para dispositivos de mano como teléfonos móviles y PDA hasta sistemas para grandes equipos con muchos procesadores y capaces de gestionar grandes cantidades de memoria central.

Vocabulario

GPL o **Licencia Pública General GNU:** es una licencia creada por la Free Software Fundation orientada a proteger la libre distribución, modificación y uso de software.

B. UNIX y distribuciones GNU/Linux

UNIX es el sistema operativo en tiempo real por antonomasia y máximamente flexible. Hay muchas marcas de UNIX, lo que conduce a una cierta complicación. Podemos encontrar versiones de UNIX de 32 y de 64 bits; de hecho, UNIX se adelantó a Windows en el soporte de sistemas de 64 bits.

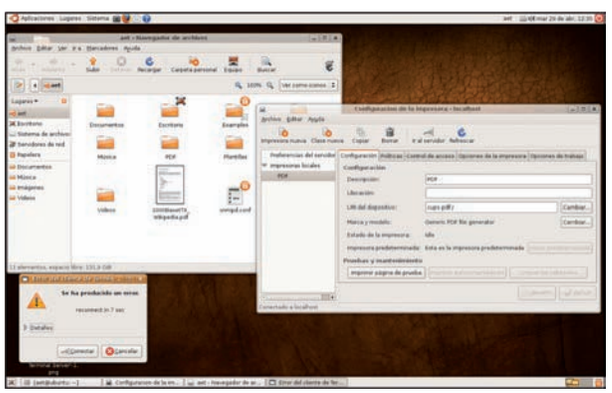


Fig. 3.2. *Ejemplo de escritorio gráfico GNOME de la distribución Ubuntu de Linux.*

GNU/Linux es un sistema operativo que sigue la tecnología de UNIX pero que se distribuye gratuitamente **bajo licencia GPL** (GNU *Public License*). Algunas compañías se dedican a comercializar distribuciones de GNU/Linux, es decir, se dedican a reunir los componentes del sistema junto con muchas aplicaciones y cobran por esta distribución, por el servicio que prestan y por las aplicaciones que no son del sistema y que ellas mismas programan o adquieren a terceros.

Aunque formalmente debe decirse GNU/Linux, habitualmente se le suele llamar simplemente Linux (nombre del kernel o del sistema operativo).

Cada distribución de Linux también tiene sus versiones cliente y sus versiones servidor. Aunque el núcleo de sistema es el mismo para ambas versiones, el número de componentes que lo acompañan varía dependiendo de si se trata de la versión de cliente o la versión de servidor.

Es muy habitual que en las distribuciones de servidor no se incorpore el sistema gráfico del sistema para que este no consuma recursos innecesarios. En cambio, en las versiones cliente la interfaz gráfica es muy importante para hacer más grato el trabajo de los usuarios finales.

La tecnología de red nativa de UNIX y de Linux es TCP/IP; sin embargo, para mejorar la interoperabilidad de estos sistemas, se les incorpora software con las pilas de otros protocolos como los de Microsoft o los de Novell NetWare.

Actualmente hay muchas distribuciones de Linux: **Ubuntu, Red Hat, SUSE, Mandrake, Debian, Fedora,** etc. Lo más básico y a la vez operativo de estas distribuciones se puede descargar gratuitamente de Internet. En la página **http://es.wikipedia.org/wiki/Anexo:Distribuciones_Linux** hay una clasificación de muchas de las distribuciones que se pueden encontrar, así como la dependencia de unas con otras.

Ampliación

UNIX no es lo mismo que Linux, UNIX fue primero. Linux se desarrolló partiendo de cero aunque con la filosofía tecnológica de UNIX. Sobre Linux podemos encontrar muchas aplicaciones GPL. También podemos observar diferencias entre algunas versiones de UNIX y Linux en la página: **http://www.unixguide.net/unixguide.shtml**

C. Apple Mac OS X

Mac OS X es el nombre comercial del sistema operativo de **Apple.** Mac OS X no es más que un sistema UNIX al que se le ha revestido de una interfaz gráfica muy potente y llamativa junto con muchas otras aplicaciones construidas por Apple, que le convierte en un sistema operativo fiable, robusto y eminentemente gráfico.

De nuevo, el protocolo de red nativo de Mac OS X es TCP/IP como en cualquier otro sistema UNIX, si bien Apple también ha incorporado por compatibilidad con las versiones anteriores de sus sistemas operativos la pila de protocolos **AppleTalk.** En el caso de Mac OS X, también existe una versión cliente y una versión servidor.

Fig. 3.3. *Escritorio típico de Apple Mac OS X.*

D. Novell NetWare

NetWare es el nombre del sistema operativo tradicional de **Novell,** aunque esta compañía ha entrado también desde hace unos años en el negocio de UNIX. El avance de Windows y UNIX ha hecho que los servidores NetWare tradicionales sean residuales.

La pila de protocolos nativa de Novel NetWare es SPX/IPX, pero NetWare es muy flexible y admite casi cualquier otra pila de protocolos, lo que le convierte en un sistema operativo de red verdaderamente interoperable.

Ampliación

Las redes NetWare determinan muy bien la parte de cliente y la parte de servidor, es decir, no forman redes punto a punto, sino que son auténticas redes cliente-servidor.

El servidor Novell es auténticamente propietario de Novell; sin embargo la parte cliente es una aplicación que puede residir en otros sistemas operativos anfitriones como DOS, cualquier versión de Windows, Apple y UNIX.

Laboratorio

Identificación de los sistemas operativos de cada nodo en la red

Profesionalmente hay que conservar siempre una documentación sencilla pero completa del software que opera en la red. Para desarrollar esta destreza, identifica los sistemas operativos de cada uno de los ordenadores conectados a la red, sean clientes o servidores. Junto con la marca del sistema operativo tendrás que adjuntar la versión del sistema, el idioma, los parches que tenga instalados y cualquier otra información que especifique características comerciales del sistema. Por ejemplo, una estación cliente podría correr un sistema Microsoft Windows 7 en español con Service Pack 1 o una versión Linux con distribución Ubuntu versión 11.04.

Escribe organizadamente toda esta información relativa a los sistemas para crear un inventario de software de sistemas.

Investigación

Es conveniente que los administradores de sistemas estén al corriente de las actualizaciones y nuevas versiones de cada sistema operativo que tengan instalados los equipos de la red. Conéctate a las webs corporativas de las organizaciones que fabrican o distribuyen estos sistemas para que conozcas su estructura de contenidos, especialmente las páginas de novedades y las de descargas de actualizaciones o parches de software.

También puedes encontrar información sobre estos sistemas en Wikipedia buscando: sistema operativo de red, Microsoft Windows, Mac OS X, Linux, Novell NetWare.

Vocabulario

System crash: es un fallo irrecuperable del sistema operativo provocado por un problema importante en el hardware o por un mal funcionamiento del software del sistema. En Windows se puede detectar un *system crash* cuando aparece inesperadamente una pantalla azul llena de mensajes indescifrables que proporcionan alguna información sobre la causa del error a los ingenieros de sistemas. En el argot profesional a esta pantalla se la denomina BSOD (*Blue Screen Of Death,* Pantalla azul de la muerte) en Windows o Kernel panic en Linux (Fig. 3.4). En general, para cualquier sistema operativo se habla de que el sistema se ha «colgado» o se ha «quedado piedra». Un *system crash* solo se puede recuperar arrancando de nuevo el ordenador desde su secuencia inicial.

Claves y consejos

Conviene visitar frecuentemente la sede web de los fabricantes de dispositivos por si hubieran publicado alguna actualización de los controladores utilizados por el hardware de nuestros equipos.

Actualizar un controlador es una operación que entraña algún riesgo. Para disminuir este riesgo, es importante hacer siempre una copia de seguridad del sistema, aunque muchos sistemas operativos permiten volver a la configuración anterior si algún controlador recién instalado provoca problemas de inestabilidad.

1.2. Componentes del sistema

El sistema operativo es como el director de orquesta que organiza todos los recursos disponibles tanto de hardware como de software en un sistema informático. Partiendo de esta metáfora, se nos hace evidente la complejidad que globalmente tiene cualquier sistema operativo y, en particular, la mayor parte de sus componentes.

A. Controlador del adaptador de red

Es el software que hace que el sistema operativo pueda comunicarse con el hardware de la tarjeta de red. Aunque el sistema operativo suele disponer de muchos controladores, lo habitual es que el fabricante del adaptador lo suministre en un CD o se pueda descargar de Internet.

Es muy importante que el controlador de un dispositivo sea el apropiado. Los fallos de software de un controlador suelen causar situaciones de ***system crash,*** que ocasionalmente son irrecuperables, especialmente si el controlador problemático es indispensable para el arranque del sistema.

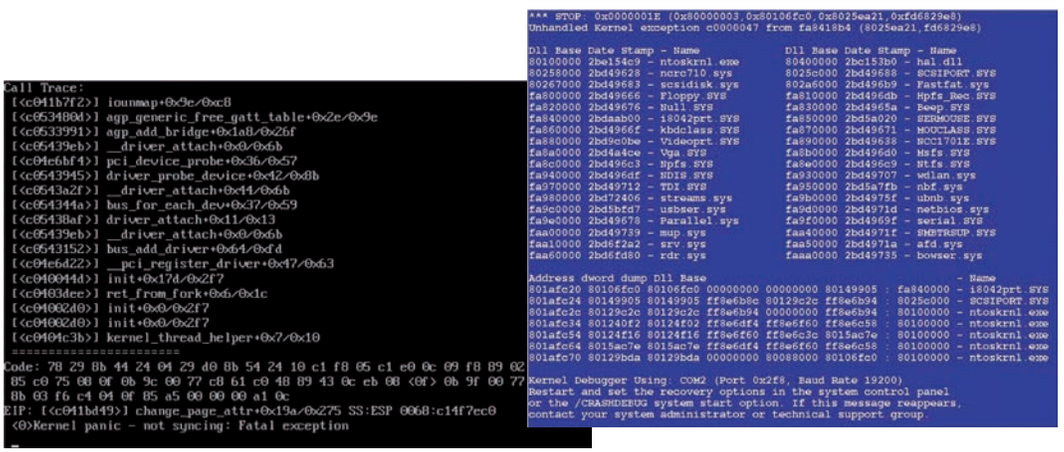


Fig. 3.4. *Pantallas de* kernel panic *(abajo, izquierda) y BSOD (arriba, derecha) que son la manifestación de que el sistema ha producido un* system crash.

Para evitar este tipo de problemas, algunos sistemas operativos permiten el arranque de los mismos con una configuración mínima. En el caso de Windows, por ejemplo, podemos arrancar el sistema en el modo de prueba de fallos, accesible desde la tecla F8 en tiempo de arranque del ordenador.

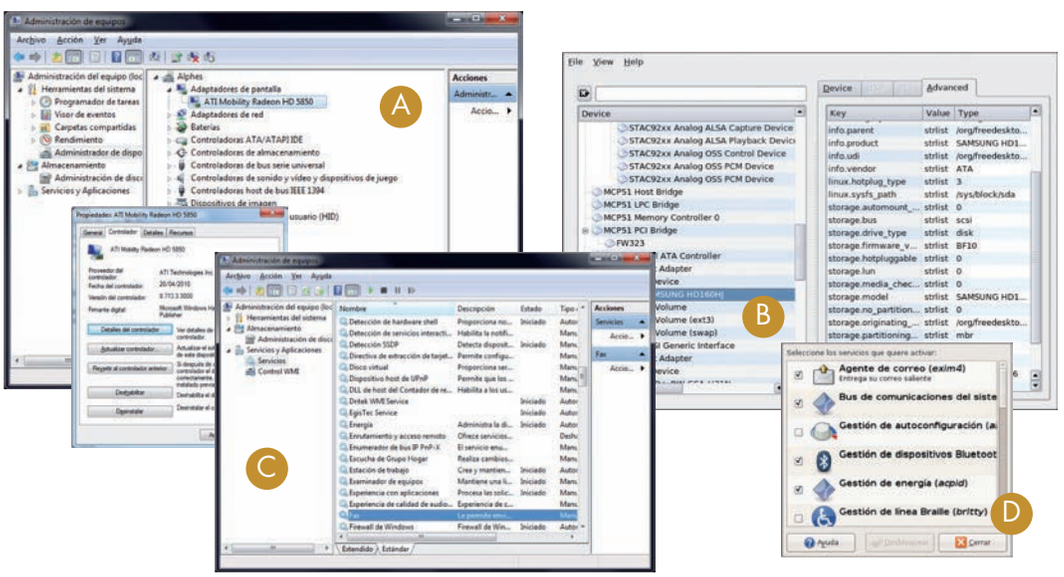


Fig. 3.5. *A) Administrador de dispositivos en Windows 7 y ficha de propiedades del dispositivo desde el que se puede actualizar el controlador o ser revocado una vez instalado. B) visor de dispositivos en Linux. C) Ventana de administración de equipo en Windows 7 abierto por la ficha de servicios. D) Administrador de arranque y parada de servicios en Ubuntu.*

B. Servicios de red

Un servicio en un sistema operativo es una tarea que se está ejecutando en ese sistema sin necesidad de un terminal (decimos que corre en *background* o, en el mundo Linux, «que es un demonio») y que proporciona una utilidad determinada. Los clientes de ese servicio realizarán sus peticiones al servicio a través de los procedimientos de comunicación soportados por el sistema operativo.

Un servicio de red es aquel que admite que las peticiones vengan a través de la red de área local. Ejemplos de servicios de red en sistemas operativos podrían ser los componentes de software que hacen que un sistema sirva ficheros o sirva impresoras, que hace que unos clientes se sirvan del acceso Internet que tiene otro nodo de la red (servicio proxy) o el elemento encargado de traducir los nombres Internet a direcciones IP equivalentes (servicio DNS).

Ampliación

En el caso de TCP/IP, a los servicios de red se accede a través de los sockets (elementos de software de comunicaciones) que asocian un número de puerto de comunicaciones y un protocolo a un servicio de red, de modo que toda comunicación de la red con el servicio se lleva a cabo a través del socket.

C. Pilas de protocolos

Con este nombre denominamos a las familias de protocolos que instalaremos en el sistema operativo. Algunas pilas de protocolos comunes son TCP/IP, SPX/IPX, NetBeui y AppleTalk.

Las pilas de protocolos se instalan con el software del sistema operativo y proporcionan su funcionalidad a través del núcleo del sistema operativo, especialmente si es la pila nativa del sistema, o a través de los servicios de red.

En otras ocasiones, las necesidades de interoperabilidad con otros sistemas exigirán que añadamos otras pilas de protocolos o servicios de red que se escapan del sistema operativo estándar. Por ejemplo, si un usuario propietario de una Palm desea sincronizarla con su correo electrónico residente en su PC de escritorio, necesitará software de comunicaciones entre la Palm y el PC que permita que se comuniquen entre sí añadiendo la funcionalidad de sincronización de datos de correo: esto se puede llevar a cabo haciendo que los dos dispositivos hablen TCP/IP o instalando en alguno de los dos dispositivos la pila de protocolos nativa del otro.

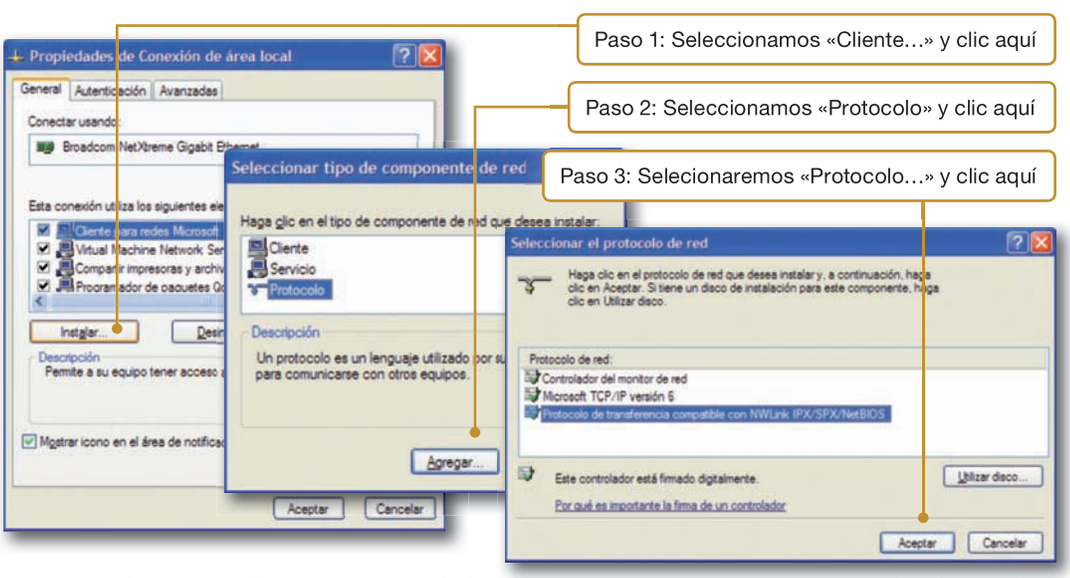


Fig. 3.6. *Fichas en Windows XP para añadir la pila SPX/IPX a un sistema que ya tiene la pila TCP/IP.*

CEO

SMR_RL_AAbad_03_MantenimientoSistema.docx
Documento que contiene información sobre:
1. Actualizaciones del sistema.
2. Caso práctico: utilización de MSINFO para identificar hardware y software.

Truco

Ocasionalmente tendremos que instalar algunas pilas de protocolos nuevas que no incorpore el sistema operativo. Por ejemplo, esto es una situación común en algunas impresoras de red que requieren protocolos de comunicación especiales. En estos casos, el fabricante de la impresora nos debería proporcionar tanto el software como los procedimientos de instalación en cada sistema operativo de red.

Actividades

1. En la tabla siguiente, relaciona el nombre de los sistemas operativos (a la izquierda) con el de las compañías fabricantes o el modelo de licencia (a la derecha).

1. Windows 7	A. GPL, GNU Public License
2. Linux	B. Microsoft
3. Windows Server 2008 R2	C. Apple
4. Mac OS X	D. Novell
5. Windows XP	
6. NetWare	

2. ¿Pueden convivir varias pilas de protocolos sobre la misma tarjeta de red? Razona la respuesta.

3. Cita las razones que conozcas por las que es conveniente actualizar frecuentemente el software de los sistemas operativos.

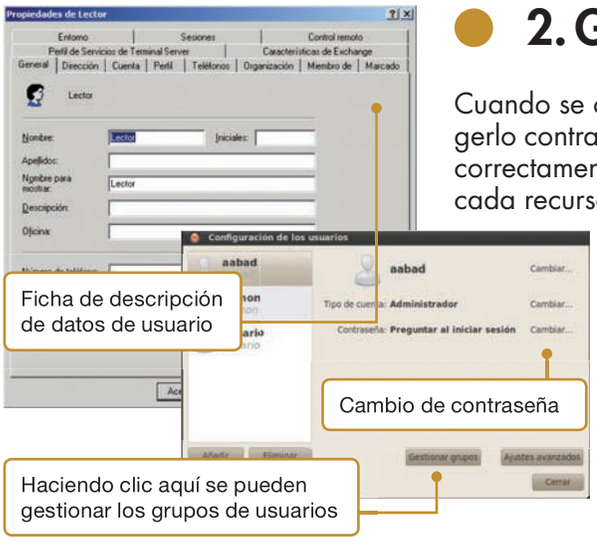


Fig. 3.7. *Ficha de creación de un nuevo usuario en un Directorio Activo de Windows, a la izquierda. Gestor de usuarios y grupos en Linux, a la derecha.*

2. Gestión de usuarios, derechos y accesos

Cuando se comparte un recurso en la red, la norma más básica de seguridad es protegerlo contra accesos indebidos. Para ello, los usuarios de la red deben ser identificados correctamente. Después, a cada usuario se le asignarán sus permisos de acceso sobre cada recurso.

2.1. Cuentas de usuario y de grupo

Las cuentas de usuario son el modo habitual de personalizar el acceso a la red. Toda persona que utilice la red con regularidad debe tener una cuenta de acceso. Para que el control de este acceso sea bueno, las cuentas deben ser personales (dos usuarios no deben compartir la misma cuenta).

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

2.2. Derechos de acceso y permisos

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

Cada recurso, servicio o utilidad tiene una información asociada que indica quién tiene y quién carece de privilegios sobre ellos.

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

1. Se determina el permiso de acceso sobre el servicio de red, por ejemplo, se puede asignar el permiso de poderse conectar a un disco de un ordenador remoto. Esto evita que se puedan abrir unidades remotas de red sobre las que después no se tengan privilegios de acceso a los ficheros que contiene, lo que podría sobrecargar al servidor.
2. Deben configurarse los permisos de los ficheros y directorios (o carpetas) que contiene ese servicio de red.

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

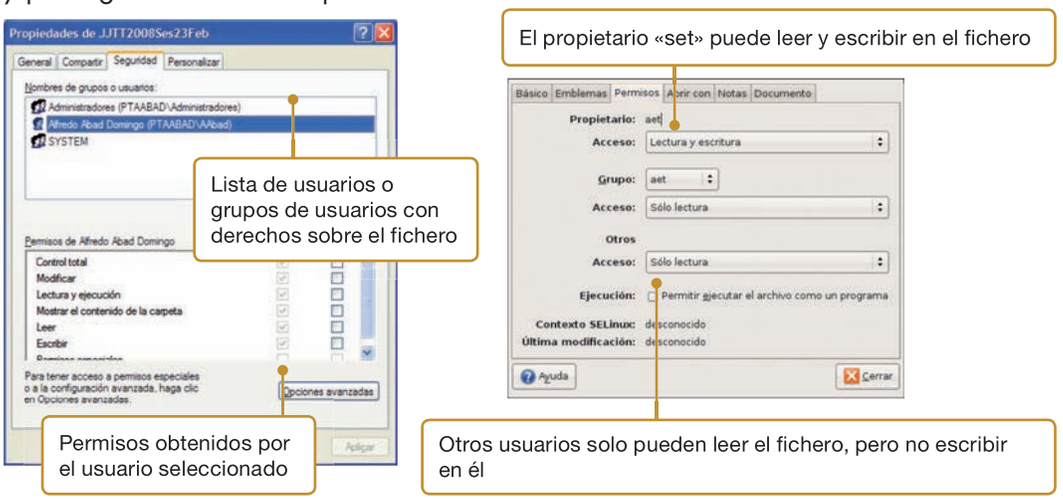


Fig. 3.8. *Configuración de privilegios sobre ficheros y carpetas en Windows y en Linux.*

Ampliación

Los derechos se refieren a operaciones propias del sistema operativo, por ejemplo, el derecho a hacer copias de seguridad. Sin embargo, un permiso se refiere al acceso a los distintos objetos de red, por ejemplo, derecho a leer un fichero concreto. Los derechos prevalecen sobre los permisos, por ejemplo, un operador de consola tiene derecho para hacer una copia de seguridad sobre todo un disco; sin embargo, puede tener restringido el acceso a determinados directorios de usuarios porque se lo niega un permiso sobre esos directorios: podrá hacer la copia de seguridad, puesto que el derecho de backup prevalece a la restricción de los permisos sobre los ficheros y carpetas concretos.

CEO

SMR_RL_AAbad_03_AdministracionCentralizada.docx

Documento que contiene información sobre:

1. Administración centralizada de la red.
2. Active Directory de Microsoft.

2.3. Notificación de errores

Una vez realizada la instalación y configuración del sistema operativo de red, debemos conducirlo al régimen de explotación, es decir, tenemos que ponerlo a producir.

Tan importante o más que una correcta configuración es el mantenimiento del sistema, que podemos definir como los procedimientos que nos permiten que el sistema operativo funcione correctamente a lo largo del tiempo, tratando de solucionar todos los problemas que surjan. Una parte muy importante del mantenimiento del sistema es la **auditoría del sistema.**

Vocabulario

Auditoría del sistema: es la configuración de alarmas que nos adviertan del estado del sistema en todo momento. De este modo, el sistema irá dejando registro de cuantos errores o acontecimientos ocurran en él.

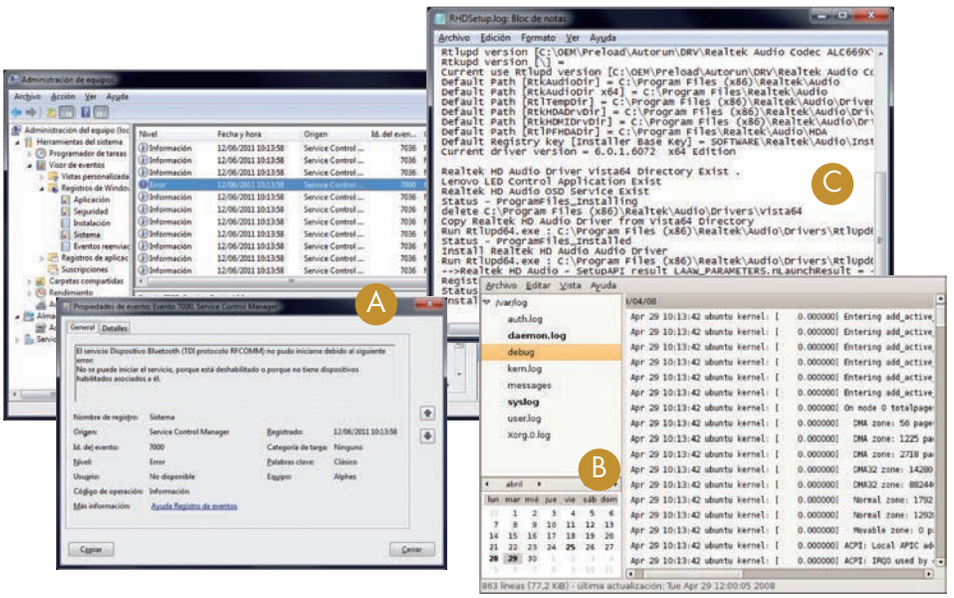


Fig. 3.9. A) Secuencia del visor de sucesos de Windows 7 y ventana descriptora de evento. B) Listado de eventos en Linux. C) Ejemplo de un fichero de log procedente de una instalación y abierto con el bloc de notas.

En la Fig. 3.9 se puede ver el visor de sucesos de Windows. Se ha seleccionado un evento que produjo un error en el sistema y este nos informa de que el dispositivo Bluetooth no ha podido iniciarse.

Los sistemas de notificación de los sistemas operativos suelen registrar la información en unos ficheros de texto denominados logs, que normalmente se pueden abrir con cualquier editor de caracteres o procesadores de texto (C).

Claves y consejos

Es muy importante registrar solo la información significativa. Cualquier sistema puede tomar nota de multitud de sucesos, pero si registramos demasiados, luego no seremos capaces de analizarlos y el registro no nos servirá para nada.

Algunas aplicaciones más avanzadas son capaces de dejar registros en tablas de bases de datos desde las que posteriormente se pueden realizar consultas o hacer análisis estadísticos y representaciones gráficas.

Actividades

4. ¿Podrías argumentar razones por las que interesa que cada usuario de una red tenga su propia cuenta de acceso identificada por su nombre de usuario?

5. ¿Por qué puede interesar que los usuarios que tengan el mismo perfil laboral pertenezcan a un mismo grupo de usuarios en el sistema operativo servidor?

6. Ensaya los procedimientos de gestión de usuarios creando unos cuantos usuarios en un sistema a los que proporciones propiedades diferentes. Prueba que estas cuentas han sido correctamente creadas iniciando una sesión en el equipo con cada cuenta recién creada. Ahora establece unos cuantos grupos de usuarios y asigna las cuentas anteriormente creadas a estos nuevos grupos.

7. Crea algunas carpetas en el disco duro de una estación de trabajo. Ahora realiza una asignación de permisos sobre esas carpetas a los usuarios y grupos creados en el ejercicio anterior. Comprueba que la asignación de permisos es correcta, es decir, que si a un usuario o a un grupo se le ha asignado solo el permiso de lectura sobre una carpeta, no podrá escribir sobre ella, si bien podrá leer la información contenida en ella.

8. En un sistema Windows, visualiza las distintas páginas del visor de sucesos e identifica los errores que se han producido en el sistema. El código numérico del suceso identifica el evento producido. Puedes investigar en Internet por qué se producen los errores que estás visualizando. Puedes empezar tu investigación buscando este código numérico en la web **http://www.eventid.net.**

Seguridad

IP es un protocolo sin conexión, por lo tanto, carece de seguridad en la entrega de paquetes. Cuando una comunicación que utiliza el protocolo IP necesita seguridad en la transferencia de paquetes de datos, esta debe ser proporcionada por otro protocolo de capa superior.

Ampliación

Cada una de estas funciones da origen a una subcapa, la primera función es propia de la subcapa de control de acceso al medio o **MAC** *(Media Access Control)*, la segunda lo es de la subcapa de control de enlace lógico **LLC** *(Logical Link Control)*, aunque normalmente esta subcapa toma el nombre de la capa OSI que la incluye: enlace de datos o **DLL** *(Data Link Layer)*.

3. La familia de protocolos TCP/IP

Por su frecuencia de uso, debemos detenernos especialmente en los protocolos que constituyen esta familia, especialmente en el protocolo IP, en el nivel de red, y el protocolo TCP, en la capa de transporte. Hay muchos más protocolos, pero la importancia de estos dos ha hecho que a toda la arquitectura de protocolos utilizados tanto en sistemas UNIX, como actualmente en muchos otros sistemas, se le llame familia de protocolos TCP/IP.

3.1. Los protocolos básicos en TCP/IP

La arquitectura TCP/IP no se fija en el nivel 2 de OSI, lo asume en lo que llama nivel de red, pero las instalaciones habituales de redes TCP/IP utilizan redes Ethernet en el nivel 2 de OSI.

El nivel de enlace asegura una conexión libre de errores entre dos ordenadores de la misma red. Fundamentalmente organiza los bits en forma de tramas y los pasa a la capa física para que sean transmitidos al receptor a través del medio de transmisión.

Cabe distinguir dos funciones en esta capa:

- Como en muchas redes de área local los canales están compartidos por muchos nodos, ¿cómo saber que el canal está libre? Y si lo está, ¿cómo sabe un nodo si puede o no apropiarse de los recursos de la red?
- Puesto que los bits deben ser agrupados en tramas, ¿cómo confeccionar esas tramas? Además, ¿cómo saber si las tramas recibidas son correctas?

Aunque TCP/IP no sigue la arquitectura OSI, se pueden establecer paralelismos como los que aparecen en la Fig. 3.10.

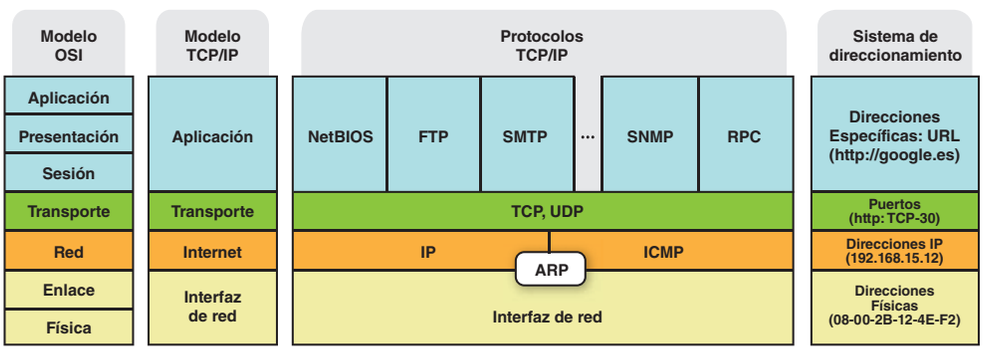


Fig. 3.10. *Estructura de capas de la arquitectura TCP/IP y su relación con OSI. Se especifican algunos ejemplos de protocolos en cada capa y un ejemplo del sistema de direccionamiento utilizado en cada nivel.*

CEO

SMR_RL_AAbad_03_NivelAccesoMedio.docx
Documento que contiene información detallada sobre funciones y protocolos utilizados en el nivel 2 de OSI.

Vocabulario

Bloque de datos: conjunto de datos que posee una estructura interior perfectamente definida.
Segmento: es el bloque de datos definido en el nivel de transporte (nivel 4 de OSI).
Paquete: es el bloque de datos propio del nivel de red (nivel 3 de OSI).
Datagrama: es un tipo de paquete (nivel 3) utilizado en servicios de comunicaciones sin conexión.

A. Protocolo IP

IP (*Internet Protocol*) es el protocolo de nivel de red en ARPANET, el sistema de comunicaciones que tradicionalmente han utilizado los sistemas UNIX y que nació a principios de los años 80. Lo más relevante de IP para el administrador de red es que proporciona un sistema de direcciones para que cada nodo de la red quede identificado por una dirección de cuatro números enteros separados por puntos (o 32 bits) denominada dirección IP o de nivel 3, para distinguirla de la dirección MAC (física) o de nivel 2 que se compone de 12 dígitos hexadecimales.

El protocolo IP acepta **bloques de datos** procedentes de la capa de transporte (por ejemplo, desde el protocolo TCP que opera en el nivel de transporte) de hasta 64 Kbytes. Cada bloque de datos, que en este nivel se denominan **segmentos,** debe ser transferido a través de la red **(Internet)** en forma de **datagramas.** Para llevar a cabo este transporte, normalmente la capa de red debe fraccionar los datagramas en un conjunto de **paquetes** IP, que deben ser ensamblados en el destino para que el mensaje sea al final reconstruido con fidelidad. Al ser IP un protocolo sin conexión, cada paquete puede seguir una ruta distinta a través de la internet. El protocolo de capa superior (TCP) será el encargado de la gestión de errores.

B. Protocolo ICMP

ICMP (*Internet Control Message Protocol,* Protocolo de mensajes de control entre redes) es un protocolo que expresa en un único paquete IP algún evento que se produce en la red. Por tanto, se trata de un protocolo de supervisión. Cualquier red TCP/IP debe utilizar el protocolo ICMP.

En la dirección **http://es.wikipedia.org/wiki/Internet_Control_Message_Protocol** puede encontrarse el formato de los paquetes ICMP así como detalles del funcionamiento orgánico del protocolo.

C. Protocolo TCP

TCP (*Transmission Control Protocol* o protocolo de control de transmisión) fue especialmente diseñado para realizar conexiones en redes inseguras. TCP es un protocolo de capa de transporte adecuado para proporcionar seguridad a IP.

La seguridad del protocolo TCP le hace idóneo para la transmisión de datos por sesiones, para aplicaciones cliente-servidor y para servicios críticos como el correo electrónico.

La seguridad en TCP tiene un precio que se manifiesta en forma de grandes cabeceras de mensajes, y de la necesidad de confirmaciones de mensajes para asegurar las comunicaciones. Estas confirmaciones generan un tráfico sobreañadido en la red que ralentiza las transmisiones en beneficio de la seguridad.

Los puntos de acceso al servicio (SAP de OSI) en la capa de transporte en TCP/IP se llaman **sockets** o conectores TCP/IP y son extraordinariamente útiles en la programación de aplicaciones de red.

Detrás de cada socket activo se implanta un servicio de red. Cuando alguien en la red requiere de ese servicio, manda mensajes al socket o puerto que identifica a ese servicio. Algunos servicios tienen necesidad de más de un socket para su funcionamiento. Por ejemplo, 80 es el puerto que identifica las peticiones de red hacia un servidor web.

D. Protocolo UDP

UDP (*User Datagram Protocol* o protocolo de datagrama de usuario) es un protocolo de transporte sin conexión, es decir, permite la transmisión de mensajes sin necesidad de establecer ninguna conexión y, por tanto, sin garantías de entrega. Actúa simplemente como una interfaz entre los procesos de los usuarios de la red y el protocolo IP. Se utiliza en transmisiones rápidas que no necesitan seguridad en la transmisión.

UDP no impone el uso de confirmaciones puesto que su objetivo no es la seguridad y esto hace de él un protocolo de transporte de mucho mayor rendimiento que TCP, y también más inseguro.

En la Tabla 3.1 se pueden observar algunas de las características que diferencian a TCP de UDP, a pesar de que ambos operan en el nivel 4 equivalente del modelo OSI o capa de transporte en el modelo TCP/IP.

TCP	UDP
Es un protocolo confiable	No es confiable
Orientado a la conexión	No establece una conexión inicial
Lleva gestión de las retransmisiones y control de flujo	No gestiona restransmisiones
Secuencia numéricamente los segmentos (paquetes de datos enviados o recibidos)	No gestiona un secuenciamiento de segmentos
Admite segmentos de acuse de recibo	No incorpora acuse de recibo

Tabla 3.1. *Diferencias sustanciales entre TCP y UDP.*

Ampliación

En ICMP son posibles, entre otros, mensajes como los siguientes:

- Destino inalcanzable. Se utiliza cuando una subred se da cuenta de que no puede alcanzar otra red solicitada por un datagrama IP, o bien, es alcanzable, pero no en las condiciones especificadas en el paquete IP.
- Tiempo excedido. El campo contador del tiempo de vida de un paquete IP ha descendido hasta 0 y ha sido drenado (retirado) de la red.
- Problemas en parámetros. El valor asignado a un parámetro de una cabecera IP es imposible. Esto suele determinar un error en la transmisión o en las pasarelas de la red.
- Enfriar fuente. Este mensaje se envía a un transmisor para que modere la velocidad de transmisión de paquetes.

Ampliación

TCP acepta bloques de datos (TPDU, *Transport Protocol Data Unit*) de cualquier longitud, procedentes de las capas superiores o de los procesos de los usuarios, y los convierte en fragmentos de 64 Kbytes como máximo que pasa a la capa de red, quien a su vez puede volver a fraccionarlos para su transmisión efectiva. Cada uno de los bloques de datos –frecuentemente se les denomina **segmentos**– se transmite como si fuera un datagrama separado con entidad propia. TCP es el responsable de ensamblar los datagramas recibidos por el receptor, ya que la red IP puede desordenarlos al utilizar caminos diversos para alcanzar su destino. IP no garantiza que los datagramas lleguen a su destino, por lo que es necesaria una entidad superior (TCP) que se encargue de ello a través de un sistema de temporizadores y retransmisiones en caso de problemas.

Ampliación

También existe el protocolo RARP *(Reverse ARP)*, que es el protocolo inverso del ARP, es decir, localiza la dirección lógica de un nodo a partir de la dirección física del mismo. Fundamentalmente es utilizado en estaciones de trabajo sin disco, que han conseguido su sistema operativo a través de la red.

Vocabulario

Dirección MAC o **dirección física:** es la dirección lógica de una interfaz de red en el nivel 2. Se compone de 12 cifras hexadecimales.

Investigación

En **http://personales.upv.es/rmartin/Tcpip/cap02s01.html** tienes unas descripción de la familia de protocolos TCP/IP y de cómo se relacionan entre sí algunos de ellos. Interesa que leas este documento o alguno similar para que te habitúes a asociar correctamente los niveles de la familia de protocolos TCP/IP con los protocolos concretos que se utilizan en cada nivel. También puedes ayudarte de la página de Wikipedia localizada por la voz «familia de protocolos de Internet».

E. Protocolo ARP

ARP (*Address Resolution Protocol* o protocolo de resolución de direcciones) no es un protocolo relacionado directamente con el transporte de datos sino que complementa la acción del TCP/IP pasando desapercibido a los ojos de los usuarios y de las aplicaciones de la red.

Como el protocolo IP (equivalente al nivel 3 del modelo OSI) utiliza un sistema de direccionamiento que utiliza el sistema operativo que no tiene nada que ver con las **direcciones MAC** (nivel 2 OSI) que utilizan las tarjetas de las redes de área local, hay que arbitrar un mecanismo de asignación de direcciones IP (cuatro números separados por puntos) a direcciones MAC propias del nivel de enlace. De esto se encarga el protocolo ARP, que funciona del siguiente modo:

Cuando un host quiere transmitir un paquete IP necesita averiguar la dirección MAC del host destinatario cuya dirección es la dirección de destino del campo «dirección de destino» del paquete IP. Para ello genera un paquete de petición ARP que difunde por toda la red. Todos los nodos de la red detectan este paquete y solo aquel host que tiene la dirección IP encapsulada en el paquete ARP contesta con otro paquete ARP de respuesta con su dirección MAC. De este modo el host emisor relaciona dirección IP y dirección MAC, guardando estos datos en una tabla residente en memoria para su uso en transmisiones posteriores.

Puede encontrarse más información detallada sobre este protocolo en la dirección **http://es.wikipedia.org/wiki/Address_Resolution_Protocol.**

3.2. El direccionamiento de red en TCP/IP

El sistema de direccionamiento IP es muy peculiar y ampliamente aceptado por la comunidad mundial. Cada dirección IP consta de 32 bits agrupados en grupos de 8 bits. Una dirección IP se expresa con cuatro números decimales separados por puntos. Cada uno de estos números varía entre 0 y 255, aunque hay algunas restricciones. Un ejemplo de dirección IP sería 128.100.3.67.

A. Clases de subredes

Como IP es un protocolo pensado para la interconexión de subredes, cada dirección IP codifica una red y un host dentro de esa red. Atendiendo a los primeros bits de cada dirección se averigua el tipo de subred de que se trata (en cuanto a su volumen) y de su dirección concreta. Los bits restantes codifican el host de que se trata dentro de esa subred. De las cinco clases de subredes, solo tres sirven para el direccionamiento particular de los nodos de la red (Fig. 3.11):

Fig. 3.11. *Estructura de los bits para las direcciones IP de las redes de clase A, B, C y D. Las direcciones de clase E están reservadas para aplicaciones futuras o para uso experimental.*

- **Redes de clase A.** Se codifican la subred y los 24 restantes la identificación del host dentro de esa subred. Los valores posibles para la subred varían entre 1 y 126, que coincide con el valor del primer byte de la dirección, es decir, hay 126 subredes posibles de tipo A. Cada una de ellas puede contener 16.777.214 hosts distintos. Este sistema de direccionamiento se utiliza, por tanto, para subredes muy grandes.
- **Redes de clase B.** Se caracterizan porque los dos primeros bits de la dirección son 10. Los 14 bits siguientes codifican la subred, desde 128 a 191 para el primer byte de la dirección, por tanto, son posibles 16.384 subredes de tipo B. Cada una de estas subredes puede contener 65.534 hosts distintos, los codificados por los 16 bits restantes del campo de dirección.

- **Redes de clase C.** Se caracterizan por tener sus tres primeros bits con el valor 110. Los 21 bits siguientes codifican la subred y los 8 restantes el host dentro de la subred. El primer byte de la dirección de una subred de clase C tiene un valor comprendido entre 192 y 223. Es posible codificar 2.097.151 subredes distintas de 254 hosts distintos cada una.

Cuando el campo de dirección comienza por la secuencia 1110, se entiende que los 28 bits restantes codifican una dirección de multidifusión, es decir, una dirección especial en donde el destinatario no es único (direcciones de clase D). Las direcciones que comienzan por 1111 se reservan para protocolos especiales como los de administración de grupos de Internet, multitransmisión y otras futuras implementaciones o uso experimental (direcciones de clase E). El valor 127 para el primer byte de una dirección IP está reservado para pruebas de bucle cerrado, es decir, para las comunicaciones entre procesos dentro de la misma máquina.

Al actual protocolo IP se le suele llamar IPv4 para distinguirlo de otra especificación que se empieza ahora a implantar: se trata del protocolo IPv6. Con IPv4 se utilizan direcciones de red de 32 bits, lo que es claramente insuficiente cuando todas las redes se integran entre sí como en el caso de Internet. Aunque tiene muchas más ventajas añadidas en las que aquí no entraremos, IPv6 viene a resolver este asunto, pues su sistema de direccionamiento es de 128 bits. Gran parte de los sistemas operativos modernos así como los dispositivos de red más aventajados ya vienen preparados para la migración de IPv4 a IPv6.

B. Máscaras de subred

Una **máscara** de subred es una secuencia de 32 bits que sirve para distinguir con facilidad qué parte de una dirección codifica la subred (una subdivisión o grupo de la red total) y qué parte el host. Una máscara se construye poniendo a 1 los bits que pertenecen a la subred y a 0 los bits que pertenecen a la identificación del host. Este modo de asignación permite multiplicar extraordinariamente los distintos tipos de subredes. Así una subred de clase A vendría determinada por la máscara 11111111 00000000 00000000 00000000, es decir, 255.0.0.0. Una subred de clase B tendría la máscara 255.255.0.0 (11111111 11111111 00000000 00000000). La subred de clase C tendría la máscara 255.255.255.0. Son posibles combinaciones cualesquiera de los bits para generar subredes y hosts dentro de las subredes siempre que tanto los «1» como los «0» aparezcan consecutivos.

En la Tabla 3.2 se pueden observar los significados de los diferentes códigos **CIDR** y cuántos hosts se pueden identificar en cada subred. La última columna (máscara equivalente) se refiere a la máscara equivalente al CIDR.

Frecuentemente, para facilitar la notación, suele expresarse la dirección IP en formato **CIDR** (*Classless Inter-Domain Routing,* Encaminamiento Inter-Dominios sin Clases), que consiste en escribir la dirección IP en su forma habitual (cuatro números enteros separados por 1) seguida de otro entero cuyo valor es el número de 1 seguidos de la máscara. Estos dos elementos deben ir separados por el símbolo «/». Un ejemplo de notación CIDR sería 128.100.3.67/24, que significaría que el interfaz de red que posee la dirección IP 128.100.3.67 tiene una máscara 255.255.255.0 (24 unos seguidos de otros 8 ceros) y, que por tanto, pertenece a la red 128.100.3.0 o simplemente 128.100.3.

Laboratorio

Identificación de las subredes de la instalación de red

Proseguimos en la investigación de la red de área local que es objeto de nuestro estudio particular para determinar cómo es su sistema de direccionamiento TCP/IP.

Observando las propiedades del protocolo TCP/IP en cada uno de los ordenadores de la red nos daremos cuenta de que las estaciones y servidores que se comunican entre sí comparten el mismo sistema de direccionamiento, permaneciendo ligados a la misma máscara o al menos a máscaras compatibles entre sí.

Identifica todas las subredes de la instalación de red así como los dispositivos que se encargan de comunicar las distintas subredes que hayas localizado.

CEO

SMR_RL_AAbad_03_RedesIPSocket.docx

Documento que contiene:

1. Ejemplo sobre cómo dos nodos saben que están o no en la misma red IP.
2. Ampliación del concepto de socket.

Vocabulario

Dirección IP: conjunto de cuatro números de ocho bits que identifican unívocamente la dirección de nivel 3 de un ordenador en una red TCP/IP.

Máscara IP: es una secuencia de unos y ceros, ambos contiguos, que sirve para denotar en las redes TCP/IP qué identifica la red (secuencia inicial de «1») y qué la subred o conjunto de nodos (secuencia final de «0»).

CIDR: es una mejora del sistema de direccionamiento IP que permite una mayor flexibilidad a la hora de asignar rangos de direcciones por el método de extender las clases de red.

CIDR	Clases C	Clases B	Clases A	Hosts*	Máscara
/32	1/256			1	255.255.255.255
/31	1/128			2	255.255.255.254
/30	1/64			4	255.255.255.252
/29	1/32			8	255.255.255.248
/28	1/16			16	255.255.255.240
/27	1/8			32	255.255.255.224
/26	1/4			64	255.255.255.192
/25	1/2			128	255.255.255.128
/24	1			256	255.255.255.000
/23	2			512	255.255.254.000
/22	4			1024	255.255.252.000
/21	8			2048	255.255.248.000
/20	16			4096	255.255.240.000
/19	32			8192	255.255.224.000
/18	64			16384	255.255.192.000
/17	128			32768	255.255.128.000
/16	256	1		65536	255.255.000.000
/15	512	2		131072	255.254.000.000
/14	1024	4		262144	255.252.000.000
/13	2048	8		524288	255.248.000.000
/12	4096	16		1048576	255.240.000.000
/11	8192	32		2097152	255.224.000.000
/10	16384	64		4194304	255.192.000.000
/9	32768	128		8388608	255.128.000.000
/8	65536	256	1	16777216	255.000.000.000
/7	131072	512	2	33554432	254.000.000.000
/6	262144	1024	4	67108864	252.000.000.000
/5	524288	2048	8	134217728	248.000.000.000
/4	1048576	4096	16	268435456	240.000.000.000
/3	2097152	8192	32	536870912	224.000.000.000
/2	4194304	16384	64	1073741824	192.000.000.000
/1	8388608	32768	128	2147483648	128.000.000.000

Tabla 3.2. *Descripción de los códigos CIDR. Fuente: http://www.vitessenetworks.com.mx*

3.3. Protocolos TCP/IP de nivel superior

En el nivel superior de la arquitectura TCP/IP hay una infinidad de protocolos. Aquí nos vamos a referir a los más comunes, pero existen casi tantos protocolos distintos como tipos de aplicaciones o servicios de nivel de aplicación:

- **FTP.** Es utilizado para la descarga o carga de ficheros en Internet. Define dos canales de comunicación, uno para el gobierno de esta y otro para la transferencia de datos. Pone en marcha el diálogo entre un cliente FTP y un servidor FTP.
- **HTTP.** Es el protocolo utilizado por los navegadores para el acceso a las páginas web.
- **SNMP.** Es uno de los protocolos de la familia TCP/IP utilizados para la gestión de la red. En cada entidad de la red, se habilitan unos agentes que recogen información y que envían a un gestor central desde donde se puede visualizar.
- **RPC.** Es el protocolo de la capa de aplicación en la arquitectura TCP/IP que se encarga de establecer diálogos entre las aplicaciones clientes y sus equivalentes servicios. Se trata de un protocolo básico para la arquitectura de las aplicaciones cliente-servidor.
- **SMTP.** Es el protocolo básico para el intercambio de mensajes de correo electrónico entre servidores de correo o el que usa la aplicación cliente de correo para enviar mensajes al servidor al que se conecta.
- **POP.** Es el protocolo de comunicaciones de alto nivel que se encarga de descargar mensajes de correo electrónico desde el servidor de correo en donde se encuentra el buzón a la bandeja de entrada del cliente de correo. La versión actual del protocolo POP es 3, por ello se denota como POP3.
- **IMAP.** Es un protocolo semejante a POP, pero con algunas funcionalidades añadidas que lo hacen recomendable en situaciones de congestión. Por ejemplo, permite descargar el correo electrónico solo a petición del usuario una vez leída la cabecera del mensaje.

La mayor parte de los protocolos de nivel superior tienen asociado uno o más números de puerto en sus sockets de comunicación, por ejemplo, FTP-21, HTTP-80, SMTP-25, POP-110, etc., aunque esta asociación puede ser alterada por las aplicaciones o por el administrador de la red.

Claves y consejos

Las aplicaciones de SNMP son muy útiles a los administradores de la red porque permiten la configuración de los parámetros de la red desde una consola central, además de recoger estadísticas de utilización de los recursos.

Ejemplos

Acceso desde el explorador a un servidor web

Con este ejemplo vamos a tratar de comprender cómo un explorador de Internet utiliza el sistema de direccionamiento y la tecnología de sockets asociados a puertos de comunicaciones para resolver la exploración de una página web.

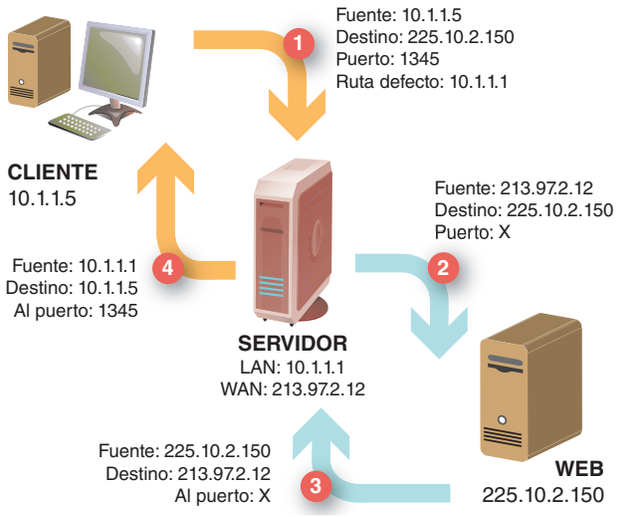


Fig. 3.12. Cliente web que accede a un servidor web a través de un encaminador.

En la Fig. 3.12 está representado el acceso de un cliente con dirección IP 10.1.1.5 con un explorador a un servidor web que reside en Internet con dirección 225.10.2.150, utilizando como intermediario un servidor que hace la función de encaminador de paquetes entre la red local en la que se encuentra el cliente e Internet en donde se encuentra el servidor. Describamos su funcionamiento.

En el paso 1, el cliente hace una petición con destino 225.10.2.150, dejando abierto el puerto 1345. Este paquete es capturado por el servidor-encaminador y envía en su nombre (dirección 213.97.2.12) el paquete al servidor web dejando abierto otro puerto «x» de su interfaz de red externo (paso 2).

El servidor web procesa la petición y devuelve (paso 3) la página a quien se la pidió que fue 213.97.2.12 por el puerto que le dejó abierto que denominamos «x».

En el cuarto paso, el encaminador pone el paquete en la red interna, enviándolo a quien le solicitó su servicio de encaminamiento por el puerto que le dejó abierto que era el 1345.

Aquí tenemos un ejemplo de un cliente que utiliza un servicio (de encaminamiento) para acceder a otro servicio informativo de páginas web.

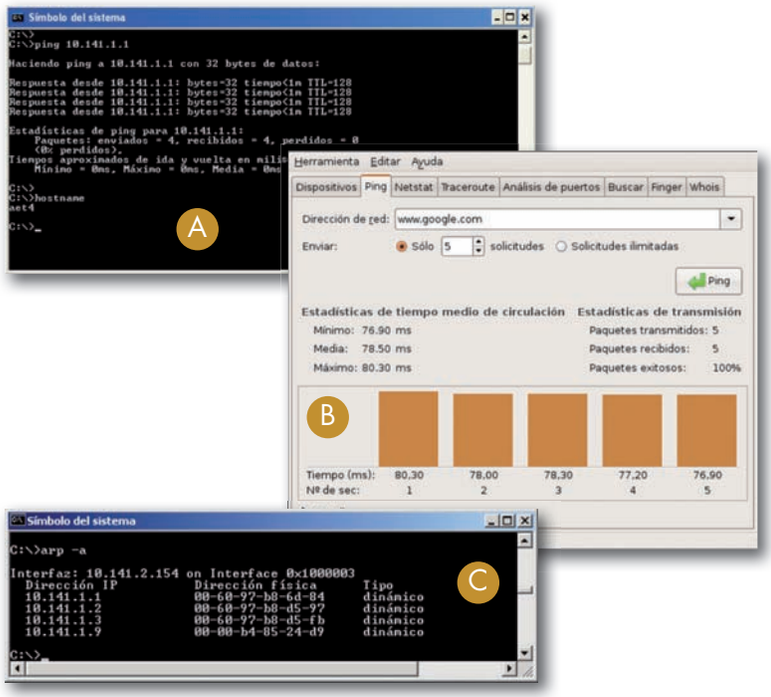


Fig. 3.13. *A) Ejecución del comando ping sobre el nodo 10.141.1.1, y verificación del nodo local con hostname en una estación Windows. B) Utilidad gráfica de ping en un sistema Linux sobre www.google.com. C) Ejecución del comando ARP.*

3.4. Utilidades propias de redes TCP/IP

Las siguientes utilidades son comunes en los sistemas UNIX. Otros sistemas operativos las incorporan en alguna medida si llevan instalado TCP/IP. El nombre exacto y los calificadores de las órdenes varían según los sistemas y las versiones. La ayuda del sistema operativo será de gran utilidad para concretar exactamente el formato de cada orden.

A. Utilidad ping

Ping (*Packet Internet Groper,* Tanteo de paquetes Internet) es una utilidad que sirve para enviar mensajes a una dirección de red concreta que se especifica como argumento con el fin de realizar un test a la red utilizando el protocolo ICMP. El nodo destinatario nos reenviará el paquete recibido para confirmarnos que se realiza el transporte entre los dos nodos correctamente. Además, proporciona información añadida sobre la red, como se puede ver en la Fig. 3.13, A y B.

Ping puede configurar varios parámetros cuando se ejecuta desde la línea de comandos, por ejemplo, es posible indicarle cuántos paquetes queremos enviar, qué información vamos a enviar con cada paquete, el tamaño de cada paquete enviado, etc. Tendremos que recurrir a la ayuda del comando ping en cada sistema para asegurarnos de la sintaxis exacta de la orden.

Hay que tener en cuenta que la utilidad ping varía dependiendo de la versión IP que ejecuta la red. Si no se especifica lo contrario, siempre se supone que se trata de la versión 4 (IPv4).

En la ejecución sobre Windows se pueden distinguir dos secciones. La primera proporciona información sobre la configuración IP del nodo: nombre (aet1), dominio al que pertenece, etc. En la segunda sección se especifican los parámetros de configuración del adaptador de red: tipo de tarjeta (3Com EtherLink XL), dirección física o MAC, dirección IP, etc.

Fig. 3.14. *Respuesta del sistema operativo de red al comando ipconfig/all en una estación de trabajo Windows (arriba). Visualización de la configuración de red para la interfaz eth1 en una estación Linux mediante ifconfig (abajo).*

B. Utilidad arp

ARP (*Address Resolution Protocol,* Protocolo de resolución de direcciones), es una utilidad sirve para asignar automáticamente direcciones IP a direcciones físicas, es decir, para gestionar el protocolo ARP. En la parte superior de la Fig. 3.13-C se interroga al sistema mediante ARP cuáles son las direcciones IP que tiene resueltas, es decir, de las que conoce su dirección física y cuál fue el tipo de asignación.

C. Utilidad ipconfig de Windows e ifconfig/iwconfig de Linux

Configura la dirección del host o bien proporciona información sobre la configuración actual. Por ejemplo, la ejecución del comando siguiente proporciona información sobre la tarjeta Ethernet 3Com EtherLink XL 10/100 PCI (Fig. 3.14, arriba).

La utilidad equivalente en Linux es ifconfig para las redes cableadas e iwconfig para las redes inalámbricas, aunque la mayor parte de las distribuciones ya permiten configurar muchos de los parámetros que admiten a través de la interfaz gráfica. La ejecución del comando «ipconfig help» en Windows e «ifconfig –h» y «iwconfig –h» en Linux nos proporcionarán la ayuda necesaria para la utilización de la orden, ejemplos incluidos. En general, cualquiera de estas órdenes tiene su propia ayuda con el calificador HELP para Windows y –h o --help para Linux.

D. Utilidad netstat

Netstat *(Network status)*, proporciona información sobre el estado de la red. El comando ejecutado en la Fig. 3.15 sobre Windows obtiene información estadística sobre los paquetes de red enviados y recibidos. Como se ve, sobre Linux, la orden puede proporcionar muchas otras informaciones como el estado de las conexiones, lo que hay al otro lado de cada conexión, etcétera.

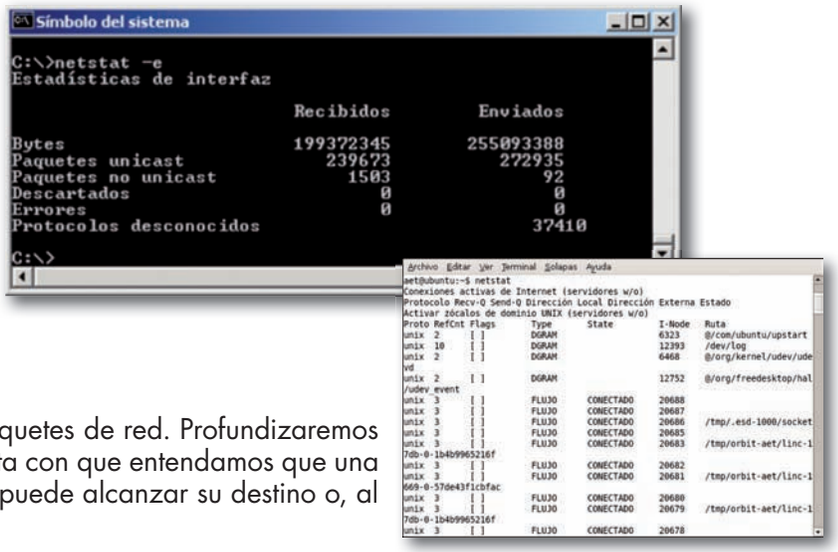


Fig. 3.15. *Respuesta del sistema al comando netstat en Windows y en Linux.*

E. Utilidad route

Sirve para determinar las rutas que deben seguir los paquetes de red. Profundizaremos en el concepto de rutas más adelante. De momento, basta con que entendamos que una ruta indica el camino apropiado por el que un paquete puede alcanzar su destino o, al menos, aproximarse a él.

Para manejar las tablas de rutas, en sistemas Windows suele utilizarse la orden ROUTE, mientras que en sistemas Linux hay una gran diversidad de órdenes y utilidades, aunque la más usual es «ip route», que admite una multitud de parámetros que deberemos consultar en cada versión para utilizarlo con propiedad.

Por ejemplo, si imprimimos las rutas disponibles para un nodo tendremos la siguiente salida (Fig. 3.16-A):

F. Utilidad tracert

Se utiliza para controlar los saltos de red que deben seguir los paquetes hasta alcanzar su destino (Fig. 3.16 B y C). Además proporciona información sobre otros parámetros de la internet. Cuando el número de saltos es 1, esto quiere decir que la red es plana, es decir, se trata de una red de área local.

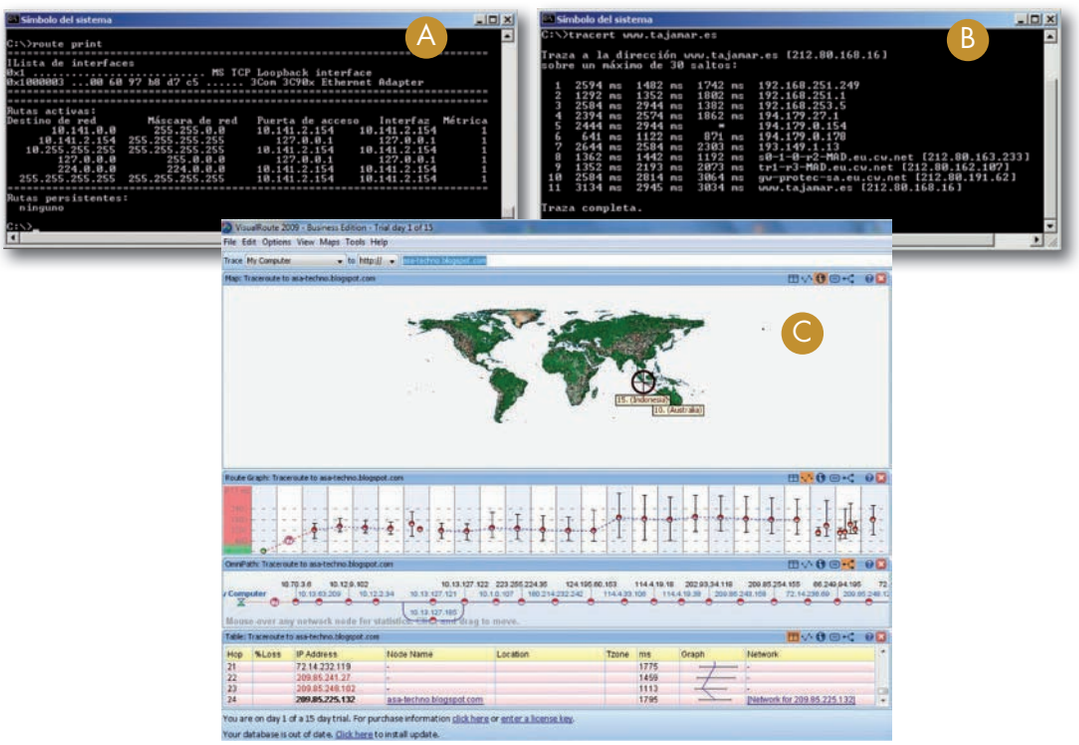


Fig. 3.16. *A) Respuesta del sistema al comando route. B) Comando tracert sobre Windows en el que se pueden observar 11 saltos. C) Utilidad gráfica VisualRoute.*

En la Fig. 3.16 A podemos apreciar tres secciones. En la primera, se especifican las interfaces de red que posee el nodo en el que se ejecuta route. En la segunda sección se describen las rutas activas en ese momento, núcleo de la tabla de enrutamiento. En la tercera sección se describen, si existen, las rutas persistentes. En Linux es habitual interrogar al sistema sobre las rutas con la orden «ip route».

Truco

Para realizar una de estas conexiones anónimas se suele utilizar como nombre de usuario la palabra «anonymous» y como contraseña, suele ser una buena costumbre teclear la dirección de correo electrónico del usuario que pretende beneficiarse del servicio ftp.

G. Utilidades ftp y tftp

La utilidad ftp sirve para intercambiar ficheros entre dos nodos de la red utilizando el protocolo FTP. FTP también tiene su parte de cliente y su parte de servidor. Cuando se ejecuta el cliente ftp, aparece el identificador de utilidad «FTP>» sobre la que se ejecutan los comandos ftp: listar, traer (bajar) o dejar (subir) ficheros, etc. Previamente a la utilización del FTP para realizar transferencias, es necesario preparar una conexión segura a través del protocolo TCP. Esto se realiza con el comando open seguido de la dirección IP o el nombre DNS del host remoto. El comando tftp es similar al ftp, más fácil de configurar, pero con menos prestaciones.

La utilización de un servidor ftp exige tener acceso al servidor a través de un nombre de usuario y una contraseña que nos asignará el administrador del sistema remoto. Muchos servidores en Internet tienen información pública a la que se accede sin necesidad de tener cuenta en el equipo, permitiendo conexiones de usuarios anónimos.

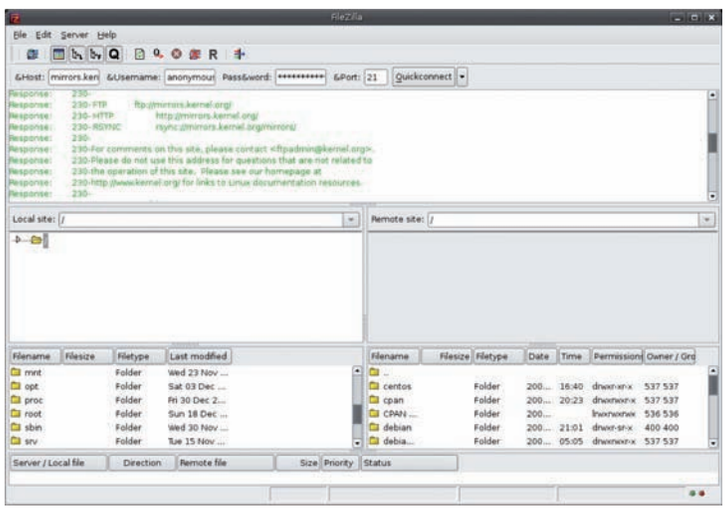


Fig. 3.17. *Ejemplo de cliente FTP gráfico.*

En la Fig. 3.17 se puede ver un ejemplo de Filezilla, un cliente gráfico típico de ftp, que tiene versiones tanto para Windows como para Linux. En la ventana izquierda aparece el sistema de ficheros local. A la derecha, una vez realizada la conexión aparecerá el sistema de ficheros remoto. Las operaciones de copiado se realizan arrastrando los ficheros o directorios desde un lado hacia el otro.

Filezilla dispone tanto de la versión cliente (la representada en la figura) como versión servidor. Es gratuita y se puede descargar desde **http://filezilla-project.org/.**

H. Utilidades telnet y ssh

Sirve para realizar conexiones remotas interactivas en forma de terminal virtual a través del protocolo de alto nivel TELNET. El comando va acompañado de la dirección IP del nodo remoto o de su dirección DNS.

Los servidores Windows implementan un servidor TELNET, que sirve sesiones en forma de ventanas emuladoras DOS a los clientes TELNET que se conectan a ellos desde su red, lo que es muy interesante para ejecutar scripts en máquinas remotas.

En el mundo Linux, la utilidad equivalente más moderna es ssh. Esta es una de las utilidades más versátiles que tiene su parte de cliente y de servidor. Puede ejecutar aplicaciones remotas, copiar ficheros, crear sesiones remotas gráficas, crear túneles de comunicación, etc. Funcionalmente, ssh puede sustituir las conexiones remotas de TELNET, pero la gran ventaja de ssh es que cifra las conexiones, por lo que es mucho más seguro que TELNET.

Investigación

En la página **http://www.guia-ubuntu.org/index.php?title=Servidor_ssh** tienes información sobre ssh. Es interesante, aunque sea más propio de sistemas que de redes, que te familiarices con esta tecnología leyendo algunos documentos técnicos. Otra página para comenzar el estudio es **http://es.wikipedia.org/wiki/Ssh**

Truco

Existen aplicaciones gratuitas que se pueden instalar en sistemas operativos de Microsoft que incorporan clientes de conexión remota como telnet, ssh y otros. Por ejemplo, PuTTY (Fig. 3.18).

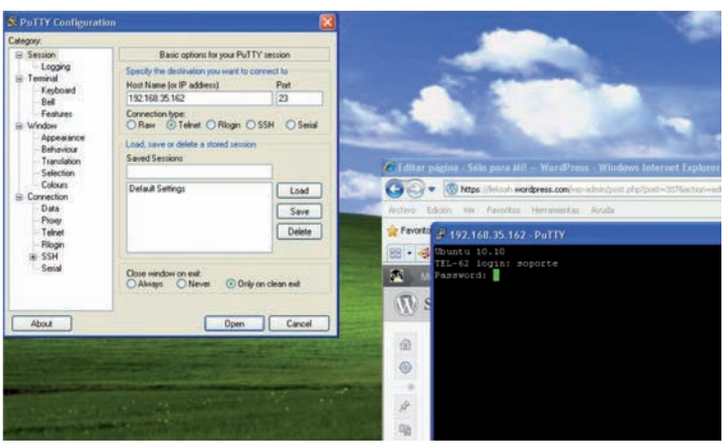


Fig. 3.18. *Ejemplo de ejecución de TELNET desde un sistema operativo de Microsoft mediante PuTTY.*

Actividades

9. Las siguientes afirmaciones ¿son verdaderas o falsas?
a) TCP es un protocolo del nivel de transporte.
b) ARP es un protocolo que sirve para resolver asociaciones de direcciones físicas en direcciones IP.
c) IP es un protocolo que se puede situar en la capa 2 de OSI.
d) Una máscara de red son cuatro números enteros cualesquiera de ocho bits cada uno separados por puntos.
e) Todos los bits puestos a «1» de una máscara de red deben estar contiguos y al principio de la máscara.
f) Dos hosts con idéntica máscara pertenecen a la misma subred.
g) Dos hosts que tienen igual la parte de dirección IP correspondiente a la secuencia de «1» de sus máscaras pertenecen a la misma subred.
h) Dos direcciones IP iguales no pueden convivir en la misma red.

10. Describe las características de las clases A, B y C para redes IP.

11. Identifica qué protocolos de la lista siguiente son específicos de la tecnología TCP/IP:

a) SNMP.	*b)* IP.	*c)* MAPI.
d) IMAP.	*e)* POP.	*f)* HDLC.
g) ARP.	*h)* X.25.	

12. Se propone el siguiente ejercicio para practicar la gestión del direccionamiento IP. Primero hay que contar con varios ordenadores en red sobre los que se tengan derechos de administración para poder modificar sus direcciones de red. A continuación, deben seguirse los siguientes pasos:
a) Elegir una máscara 255.255.255.0 (clase C) y una dirección 192.168.100.x, donde x será el número que identifique cada PC (si hubiera cinco PC, x valdría 1 en el primer PC, 2 en el segundo, etc.). Después de asignar estas direcciones y máscaras a cada PC, comprobar que todos pueden comunicarse entre sí utilizando la orden «ping destino», donde destino es cualquier PC en red.
b) Seguidamente modificar las máscaras de los PC por 255.255.0.0 (clase B). ¿Pierdes la comunicación? ¿Por qué?
c) Vuelve a la máscara 255.255.255.0 y modifica las direcciones IP de un subgrupo de PC para que sean 192.168.50.x. Comprueba ahora qué PC pueden comunicar con qué otros. Ahora observarás que tienes dos subredes conviviendo en la misma red física, con la misma máscara pero con diferentes direcciones IP: la red 192.168.100 y la 192.168.50.
d) Por último, vuelve a establecer la máscara de todos los PC como 255.255.0.0. En ese momento, has vuelto a tener una única subred (la 192.168) por integración de las dos subredes en una superior. Comprueba que al estar de nuevo todos los PC en una única subred, todos vuelven a tener comunicación entre sí.

13. Busca en Internet una herramienta de escaneo de puertos de libre distribución. Podrás encontrarla buscando «escáner de puertos» o «port scanner». Instálala en una estación de la red y ejecútala para analizar los puertos (sockets) que tiene abiertos un servidor y los servicios asociados a ellos. Si realizas esta operación contra todos los servidores de la red, podrás realizar un mapa de servicios de red.

14. Se propone el siguiente ejercicio para practicar la identificación de parámetros de red. Hemos de partir de un conjunto de PC en red con direcciones IP compatibles de modo que todos puedan responder a la orden ping.
a) Elige un PC diana contra el que vas a hacer las pruebas y otro PC cliente desde el que ejecutarás los comandos y en el que operarás tú mismo. Comprueba que la red de ambos PC está operativa.
b) Haz ping desde el PC cliente contra el PC diana. Comprueba que tienes comunicación porque la orden ping obtiene eco del destino.
c) ¿Cuál es la dirección física del PC destino? Con la orden arp –a obtendrás el listado de todas las direcciones físicas con las que el PC cliente se ha comunicado en los últimos minutos. Una de ellas será la dirección física del PC diana: la que corresponda a su dirección IP.
d) Deja pasar algunos minutos sin actividad de red entre el PC cliente y el PC diana y vuelve a ejecutar la orden arp –a. Observarás que la dirección física del PC diana ha desaparecido puesto que la tabla de direcciones arp es dinámica y se reconstruye cada cierto tiempo.

15. Para realizar este ejercicio deberás tener disponible en el laboratorio un servidor ftp básico. Cada servidor ftp admite un conjunto de calificadores para la orden ftp de los clientes que se conectan a él. También existe esta dependencia por parte de los clientes. La ayuda de la orden ftp te puede orientar sobre cómo utilizarlo.
a) Identifica en primer lugar la dirección IP del servidor ftp y asigna al cliente que vayas a utilizar una dirección compatible con la del servidor de modo que puedas establecer comunicación entre ellos con la orden ping.
b) Si el servidor ftp requiere autenticación, el administrador del servidor deberá proporcionarte una cuenta de acceso y un directorio sobre el que poder hacer cargas y descargas.
c) Abre el cliente ftp especificando la dirección URL del lugar que te haya asignado el administrador del servidor ftp (Ayuda: comando open).
d) Sube un fichero desde el PC cliente al servidor (Ayuda: comando put).
e) Desde otro cliente, conéctate al servidor ftp y trata de descargarte el fichero que subiste en el apartado anterior (Ayuda: comando get).

Caso práctico 1

Configurar el sistema de direccionamiento IP de nodos Linux y Windows

Asignar direcciones IP a los ordenadores de la red es la actividad más frecuente del administrador de red puesto que un ordenador no puede funcionar en red sin un correcto sistema de direccionamiento. Vamos a suponer que el administrador de una red tuviera que configurar un servidor y un cliente de la red. El servidor podría ser una máquina destinada a servir sus discos como carpetas compartidas en la red. El cliente podría ser el portátil de un comercial que conecta frecuentemente a la red empresarial, pero que también lo tiene que conectar a las redes de las empresas de los clientes que visita y que, por tanto, debe cambiar su direccionamiento muy a menudo.

Es posible configurar estas direcciones dinámicamente (mediante DHCP) o estáticamente. En el primer caso habrá un servicio de red (servidor DHCP) que asignará automáticamente las direcciones IP a los ordenadores de la red. En el caso segundo, será el administrador de red quien asigne manualmente la dirección a cada ordenador.

Habitualmente, los servidores llevan una dirección estática porque así es más fácil encontrar los servicios de red que provea. En el caso de los clientes, se puede utilizar un sistema dinámico que es más cómodo o el estático.

Vamos a configurar una dirección dinámica (el caso de un cliente) y una dirección estática (el caso de un servidor) tanto para Windows como para Linux.

Configurando sobre Linux

Para asignar la dirección IP acudiríamos al panel de red, que está accesible desde el menú de herramientas de sistema (su nombre exacto dependerá de la distribución que utilicemos) y nos aparecerá un panel como el de la Fig. 3.19-A.

Fig. 3.19. *Configuración gráfica de la dirección IP en Linux.*

Seleccionamos la interfaz de red sobre la que queramos operar, que en la figura es eth1, y hacemos clic sobre el botón de propiedades para que nos aparezca la ventana de la Fig. 3.19-B. Desde allí tenemos dos posibilidades:

a) Configurar el modo itinerante: esto activa el direccionamiento automático del nodo y la tarjeta de red esperará a que algún servidor DHCP le asigne automáticamente su dirección. Este sería el caso de querer configurar un cliente con direccionamiento automático.

b) Configurar una dirección estática (como aparece en la imagen). En este caso le hemos asignado al nodo la dirección 10.1.1.94, con máscara de red 255.255.255.0 y puerta por defecto 10.1.1.20.

Configurando sobre Windows

En este caso la configuración de la red es accesible desde el icono de «Red» del Panel de control de Windows.

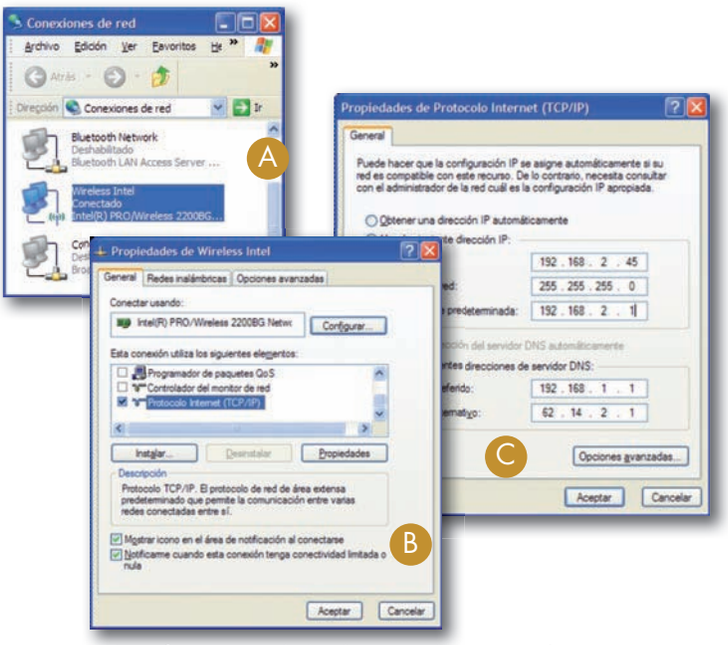


Fig. 3.20. *Configuración de la dirección IP en Windows.*

Nos aparecerá una ventana con un listado de las interfaces disponibles por el sistema (Fig. 3.20-A). Elegiremos la que nos interese (en nuestro caso es una interfaz inalámbrica denominada «Wireless Intel») y haciendo clic con el botón derecho del ratón elegiremos «Propiedades». Se desplegará la ventana de la Fig. 3.20-B, que nos presenta una lista con las pilas de protocolos y otros servicios disponibles. Seleccionaremos la pila TCP/IP y haciendo clic en propiedades nos presentará la ventana de la Fig. 3.20-C. Desde allí, tenemos dos posibilidades:

a) Si seleccionamos «Obtener una dirección IP automáticamente», le indicamos a Windows que solicite para esa tarjeta de red una dirección IP automáticamente. Sería nuestro caso de cliente.

b) Si seleccionamos «Usar la siguiente dirección IP», Windows nos iluminará los campos de dirección IP y máscara de red para que los podamos introducir manualmente. De este modo configuraríamos el servidor con dirección IP estática.

El resto de los campos no son relevantes de momento.

Según esta configuración, el servidor (sea Windows o Linux) siempre tendrá una dirección fija, fácilmente localizable por todos los usuarios de la red. En el caso del portátil del comercial, al tener configurada su dirección IP mediante un procedimiento automático, su dirección variará en función de la red a la que se conecte, pero será transparente para él.

4. Familia de protocolos en sistemas de Microsoft

Fundamentalmente Microsoft propone los tres siguientes posibles transportes que son compatibles entre sí formando hasta tres pilas de protocolos:

- Protocolo **NetBeui** (*NetBIOS Extended User Interface,* Interfaz de usuario extendida NetBIOS). Da soporte para pequeñas redes y es un protocolo de transporte muy simple y fácil de utilizar. Solo se puede aplicar a redes de área local, es decir, NetBeui es un protocolo incapaz de ser encaminado para saltar de una red de área local a otra.
- Protocolo **IPX/SPX.** Como se ha visto anteriormente, este protocolo ha sido construido por Novell para su sistema NetWare. Da soporte para redes pequeñas y medianas. Con IPX/SPX es posible un sistema básico de encaminamiento. Microsoft ha construido protocolos compatibles con IPX/SPX, que dan servicio de transporte como si se tratara de redes NetWare, por ejemplo, el protocolo NwLink.
- Protocolo **TCP/IP.** Este protocolo ha sido diseñado especialmente para poder ser encaminado entre distintas redes de área local. Es el protocolo ideal cuando en la instalación se halla presente una red de área extendida o se pretenden conectar los ordenadores de la red a Internet.

Con TCP/IP, Microsoft sigue ofreciendo a los usuarios de sus sistemas operativos la misma interfaz que utilizaba con redes NetBeui. Por ejemplo, cuando un usuario necesita acceder a un recurso de la red como una carpeta o una impresora, el nombre del recurso en la red se compone como la suma de dos literales.

El primer literal contiene el nombre del servidor dentro de la red en algún formato permitido por la red, por ejemplo: miservidor.miempresa.com. El segundo literal contiene el nombre del recurso compartido: la carpeta o la impresora. Por ejemplo: ImpresoraPlanta1.

De este modo el acceso a la impresora a través de la red se lleva a cabo con el siguiente nombre compuesto:

\\miservidor.miempresa.com\ImpresoraPlanta1

Otros sistemas operativos también pueden utilizar los recursos servidos por las redes de sistemas operativos de Microsoft. Samba, por ejemplo, es una tecnología utilizada por sistemas Linux para compartir recursos simulando las redes de Microsoft. Si un sistema Linux, con Samba instalado y configurado, brinda una carpeta a la red, otro sistema Windows en la misma red lo verá como si el servicio residiera en otro sistema Windows en vez de en Linux. De modo semejante, un sistema Linux puede aprovecharse de una carpeta servida por otro sistema Windows utilizando un cliente Samba.

Claves y consejos

A la hora de decidir qué protocolo instalar como transporte en el sistema de Microsoft se debe tener en cuenta lo siguiente:

- Si la red es pequeña y no se prevé un crecimiento considerable a corto plazo, bastaría con poner NetBeui, aunque se recomienda TCP/IP.
- Si el servidor o las estaciones con software de Microsoft deben convivir en un entorno de red en que se hayan presentes servidores NetWare, entonces conviene instalar el protocolo IPX/SPX.
- En cambio, si la red de área local debe estar conectada a Internet o debe estar muy segmentada, entonces el protocolo más apropiado es TCP/IP.

Ampliación

Microsoft permite además la incorporación de otros protocolos para conexiones específicas como el protocolo DLC (Data Link Control), protocolos AppleTalk para interconexión con redes de Apple, etc. Linux también permite la incorporación de otros protocolos que no le son nativos pero, en general y debido a la filosofía que abandera, es más reacio a integrar protocolos propietarios.

En las últimas versiones de Windows se observa un abandono paulatino del protocolo NetBeui. Esto generaría grandes problemas de compatibilidad con redes anteriores de Microsoft que tradicionalmente utilizaron este protocolo. Para resolver este problema, Microsoft ha incorporado la interfaz NetBIOS, empleada por la mayor parte de las aplicaciones construidas para usar la red con NetBeui, utilizando como transporte TCP/IP en vez de NetBeui. De este modo, las aplicaciones NetBIOS siguen funcionando pero sirviéndose de una red universal como es la red TCP/IP. De hecho, a partir de Windows XP el protocolo NetBeui no está disponible en la instalación típica del sistema operativo.

En la ventana superior de la Fig. 3.21, denominada «Propiedades de Conexión de área local», tenemos la ventana de configuración de la red en Windows. Se debe observar que tiene algunos elementos instalados. El primero que aparece en la figura, denominado «Compartir impresoras y archivos para redes Microsoft», se encarga de que los recursos locales puedan ser compartidos en la red; se trata, por tanto, de un componente servidor. No consideraremos de momento el segundo elemento de la figura.

El tercer elemento es el protocolo TCP/IP. Desde aquí se pueden configurar todos los parámetros de una red TCP/IP en Windows.

Si decidimos instalar más componentes de la red, lo que se consigue haciendo clic en el botón de instalar, nos aparecerá la ventana superior derecha. En ella vemos que podemos agregar clientes, servicios o protocolos. Un cliente nos permitiría usar los servicios de la red proporcionados por otros servidores que utilizan otras tecnologías de red. De los servicios aún no nos ocuparemos, pero si decidimos añadir nuevos protocolos entonces obtendremos la ventana inferior derecha que permite añadir entre otros protocolos, la pila del protocolo IPX/SPX utilizando NetBIOS sobre él.

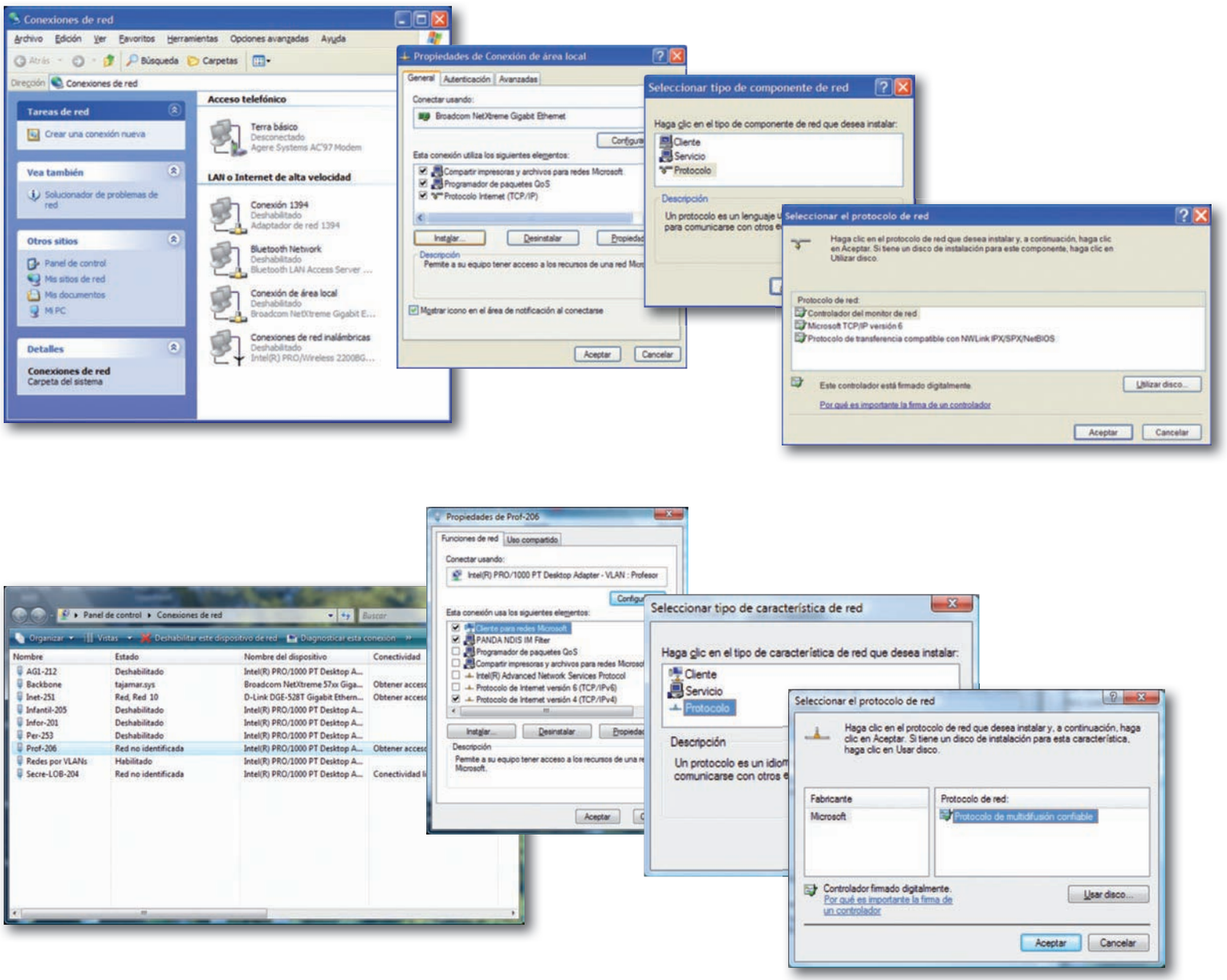


Fig. 3.21. *Secuencia de ventanas del asistente de instalación de protocolos en distintos tipos de sistemas Windows.*

Actividades

16. ¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma red? ¿Por qué?

¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma tarjeta de red? ¿Depende de la tarjeta de red o del sistema operativo?

17. Prepara unos ordenadores en red que tengan como sistema operativo alguna versión de Windows. Después sigue los siguientes pasos:

a) Asegúrate de que cada PC tiene un nombre distinto que le identifique unívocamente. Además todos deben pertenecer al mismo grupo o dominio NetBIOS. Tanto el nombre como el grupo al que pertenecen se pueden configurar desde las Propiedades de «Mi PC» (en algunas versiones de Windows, «Mi Equipo»).

b) No es necesario que estos PC ejecuten el protocolo TCP/IP, basta con NetBEUI, pero si tienen TCP/IP asegúrate de que todos comparten el mismo sistema de direccionamiento.

c) Ahora abre el explorador de Windows y abre desde él «Mis sitios de red». Investiga en las subcarpetas de la red y verás todos los servicios compartidos a la red que tienen los PC del grupo a través de NetBIOS. Ten en cuenta que solo verás aquellos servicios para los que tengas derecho desde tu cuenta de acceso a la red.

18. Entérate de los servicios de red provistos por la red de área local que estamos estudiando y prueba a realizar conexiones a estos servicios desde una estación cliente. Ensaya especialmente las conexiones a servicios de ficheros y de impresoras compartidas. Ve familiarizándote con los nombres de los servidores y de los servicios compartidos que proveen.

Caso práctico 2

Subnetting

Se hace evidente que la dirección IP de un nodo es el elemento que mejor le define tecnológicamente desde el punto de vista de la red. Es por ello muy importante adquirir una cierta soltura en los cálculos relativos a los sistemas de direccionamiento.

Para el estudio se partirá de un ejemplo sobre el que intentaremos calcular todos los parámetros de red. En concreto, se dispondrá de un nodo con dirección 192.168.15.12 con máscara de red 255.255.255.0 (o lo que es lo mismo 192.168.15.12/24 en notación CIDR) y con puerta por defecto (dirección del encaminador que le conecta a Internet) 192.168.15.254 (Fig. 3.22).

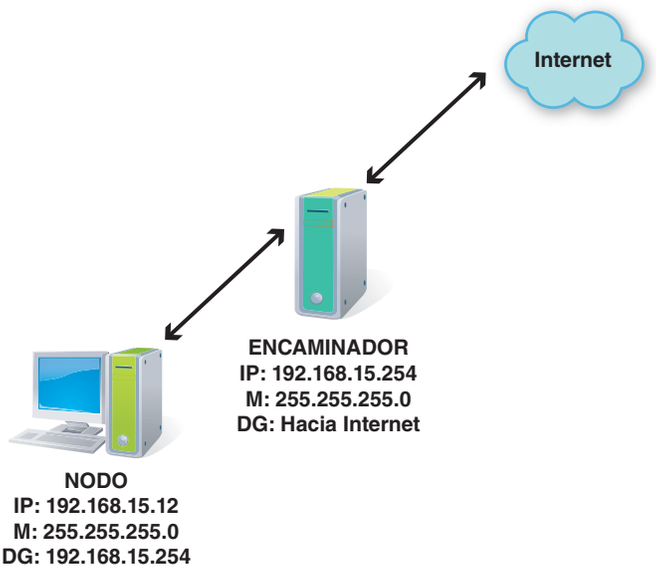


Fig. 3.22. *Ejemplo de red para el cálculo de parámetros IP.*

A. Cálculo de direcciones IP

Cálculo de la máscara de red de clase

La dirección IP del nodo (192.168.15.12) se corresponde con una red de clase C (puesto que el primer octeto está comprendido entre 192 y 233). Su máscara de red de clase es de 24 bits, es decir: 255.255.255.0, lo que en este caso se nos proporciona como dato de partida.

Cálculo de la dirección de red

La dirección de red se construye a partir de la dirección del nodo, sustituyendo los bits que codifican el host por ceros y dejando intactos los bits que codifican la red.

En este caso, como la máscara es de 24 bits, habrá que dejar intactos los 24 primeros bits y poner a cero los 8 bits restantes (los que aparecen más a la derecha en la máscara).

La dirección de red será, por tanto:
192.168.15.00000000 = 192.168.15.0

Lo que a veces se especifica simplemente como 192.168.15.0 o más sencillamente como 192.168.15.

Continúa...

Caso práctico 2

…Continuación

Cálculo de la dirección de difusión o broadcast de la red

Esta dirección se utiliza cuando un nodo quiere enviar datos a todos los nodos de su red lógica (todos los que comparten su sistema de direccionamiento y con los que él puede comunicarse directamente sin el concurso de dispositivos intermediarios).

La dirección de difusión de red se calcula también a partir de la dirección IP del nodo, dejando intactos los bits que codifican la red y estableciendo a uno los bis que codifican el host dentro de la red.

En el caso que nos ocupa la dirección de difusión será: 192.168.15.11111111 = 192.168.15.255.

Nótese que ni la dirección de red ni la de difusión pueden aplicarse a un nodo, puesto que están reservadas para esas dos funciones especiales: representar a la red (dirección de red) y representar a todos los nodos de la red (dirección de difusión).

Comprobación de que el nodo se comunica con su puerta por defecto

Al configurar la red en un nodo hay que asegurarse de que, si tiene establecida su puerta por defecto, el nodo está en la misma red lógica que su puerta, de lo contrario no se podrán comunicar entre sí.

¿Cómo saber si están en la misma red dos nodos? Es muy sencillo: calculamos la dirección de red del primer nodo, calculamos la dirección de red del segundo nodo y comprobamos que coinciden.

Si realizamos al cálculo de la dirección de red de la puerta por defecto del nodo (encaminador) siguiendo el procedimiento descrito anteriormente se tendrá lo siguiente:

Dirección de red del encaminador:
192.168.15.00000000 = 192.168.15.0

Que coincide con la dirección de red de nodo, por tanto, están en la misma red y el nodo podrá comunicarse con su puerta.

B. Subnetting

A veces interesa que la división que produce una máscara de red entre la parte de nodo y la parte de red no sea tan generosa como la que proporcionan las redes de clases (A, B y C; las direcciones de tipo D y E no intervienen en este estudio).

Por ejemplo, podría darse el caso de una empresa que ha contratado una red con direcciones IP públicas de clase C para repartir entre todos los departamentos de que consta.

Por tanto, el administrador de red de esta empresa tiene que hacer una subdivisión del direccionamiento IP de la red de clase C contratada, confeccionando a partir de esta un conjunto de redes más pequeñas y asignando cada una de ellas a los distintos departamentos. A esta operación de fraccionamiento del sistema de direccionamiento se le llama **subnetting.**

La técnica de subnetting consiste en crear máscaras de mayor número de bits puestos a uno que las que proporcionan las máscaras de clase (8, 16 y 24 bits respectivamente para las clases A, B y C).

Esta división genera un conjunto de subredes, cada una de las cuales tiene su propio sistema de direccionamiento, su nueva máscara, su dirección de red y su dirección de difusión. A partir de aquí se aprenderá a realizar estos cálculos.

Para ilustrarlo se supondrá que disponemos de las direcciones IP de la red de clase C 192.168.15.0 que tendremos que repartir en tres subrangos de red, por ejemplo, porque haya tres departamentos. A cada departamento le asignaremos una de estas subredes.

Cálculo de tres parámetros: número de bits que desplazaremos en la máscara, nueva máscara de subred (máscara adaptada) y número de subredes que conseguiremos con la división

Como partimos de una red de clase C, tomamos inicialmente una máscara de 24 bits, es decir:

255.255.255.00000000

Nos hacemos la siguiente pregunta: ¿Cuántos bits de los 8 que aparecen a la derecha de la máscara anterior tendrían que convertirse en unos para poder codificar tres subredes?

Esta pregunta exige el siguiente cálculo: tomar un número de bits (entre 2 y 6 para una red de clase C), elevar 2 a ese número y restarle 2 al resultado, es decir:

$$\text{Número de subredes válidas} = 2^{\text{Número de bits desplazados}} - 2$$

Para una red de clase B, el número de bits desplazados debe estar comprendido entre 2 y 14, mientras que para una red de clase C entre 2 y 22. La justificación de estos cálculos se comprobará más adelante.

En nuestro ejemplo, si elegimos 3 bits, tendremos que el número de subredes válidas será de 23 – 2 = 8 – 2 = **6 subredes válidas.**

Con 6 subredes válidas se pueden cubrir los tres departamentos y nos sobran otras tres subredes para usos futuros.

Continúa…

Caso práctico 2

…Continuación

Nota: Se puede comprobar que con 2 bits no hubiéramos tenido suficiente, puesto que en este caso el número de redes válidas que saldrían serían: $2^2 - 2 = 4 - 2 = 2$ (un departamento de los tres que tenemos se quedaría sin su propia subred).

Por tanto, el número de bits desplazados que hemos calculado es 3 y el número de subredes válidas en que podremos subdividir la red será de 6.

La nueva máscara de subred o máscara adaptada será 255.255.255.11100000 = **255.255.255.224.**

Cálculo del número hosts que pueden direccionarse en cada subred

En este caso el cálculo del número de hosts válidos en cada subred es similar al de subredes, pero en vez de tomar el número de bits desplazados se toman los restantes.

Para una red de clase C: $2^{8 - \text{bits desplazados}} - 2$.

Para una red de clase B: $2^{16 - \text{bits desplazados}} - 2$.

Para una red de clase A: $2^{24 - \text{bits desplazados}} - 2$.

Por tanto, en nuestro ejemplo, el número de hosts válidos en cada subred será de

Número de hosts válidos en cada subred = $2^{8-3} - 2 = 2^5 - 2 = 32 - 2 =$ **30 hosts/subred.**

Cálculo de las direcciones de red de cada subred válida

Hemos desplazado 3 bits, que ahora codifican la subred, por tanto, tenemos lo siguiente:

a) Los 24 primeros bits codifican la red: 192.168.15.

b) Los 3 bits siguientes codifican la subred: desde la 000 hasta la 111 (8 subredes, de las cuales solo 6 serán válidas). Ni la primera subred ni la última son válidas (lo que justificaremos más adelante).

c) Los 5 bits siguientes (y últimos) codifican el host dentro de la red: desde el 00000 hasta el 11111 (32 hosts en cada subred, de los cuales solo 30 son válidos). Ni el primer host ni el último son válidos (también será justificado más adelante).

¿Cuáles serán las direcciones de red de cada una de las subredes válidas?

Ponemos a cero los cinco bits de host, que aparecerán a la derecha del símbolo «,» que utilizaremos para separar los bits del último octeto:

1) Dirección de red de la primera subred: 192.168.15.000,00000 = 192.168.15.0 (no válida, puesto que coincide con la dirección de red de la red de clase C de la que partimos y si la tomamos no podremos distinguir entre la dirección de red de la clase C y de la primera subred): la descartamos.
2) Dirección de red de la segunda subred: 192.168.15.001,00000 = 192.168.15.32 (dirección de subred del primer departamento).
3) Dirección de red de la tercera subred: 192.168.15.010,00000 = 192.168.15.64 (dirección de red del segundo departamento).
4) Dirección de red de la cuarta subred: 192.168.15.011,00000 = 192.168.15.96 (dirección de red de tercer departamento).
5) Dirección de red de la quinta subred: 192.168.15.100,00000 = 192.168.15.128.
6) Dirección de red de la sexta subred: 192.168.15.101,00000 = 192.168.15.160.
7) Dirección de red de la séptima subred: 192.168.15.110,00000 = 192.168.15.192.
8) Dirección de red de la octava subred: 192.168.15.111,00000 = 192.168.15.224 (esta subred también es inválida, pero la razón se expondrá después).

Cálculo de las direcciones de difusión de cada subred válida

Hacemos lo mismo que en el apartado anterior, pero poniendo esta vez a uno los bits que codifican el host.

1) Dirección de difusión de la primera subred: 192.168.15.000,11111 = 192.168.15.31 (aunque sabemos que esta subred no sirve porque no es válida su dirección de red).
2) Dirección de difusión de la segunda subred: 192.168.15.001,11111 = 192.168.15.63 (dirección de difusión del primer departamento).
3) Dirección de difusión de la tercera subred: 192.168.15.010,11111 = 192.168.15.95 (dirección de difusión del segundo departamento).
4) Dirección de difusión de la cuarta subred: 192.168.15.011,11111 = 192.168.15.127 (dirección de red de tercer departamento).
5) Dirección de difusión de la quinta subred: 192.168.15.100,11111 = 192.168.15.159.
6) Dirección de difusión de la sexta subred: 192.168.15.101,11111 = 192.168.15.191.

Continúa…

Caso práctico 2

…Continuación

7) Dirección de difusión de la séptima subred: 192.168.15.110,11111 = 192.168.15.223.

8) Dirección de difusión de la octava subred: 192.168.15.111,11111 = 192.168.15.255 (esta subred también es inválida, porque su dirección de difusión coincide con la dirección de difusión de la red de clase C de la que partimos).

Cálculo de las direcciones IP de los nodos de cada una de las subredes válidas

Si tomamos una subred válida, por ejemplo, la primera de todas las válidas, las direcciones IP asignables a los nodos del primer departamento estarán comprendidas entre su dirección de red y la de difusión.

Por tanto, tendremos:

Primera red válida: desde 192.168.15.33 hasta 192.168.15.62 (30 nodos para el primer departamento).

Segunda red válida: desde 192.168.15.65 hasta 192.168.15.94 (30 nodos para el segundo departamento).

Tercera red válida: desde 192.168.15.97 hasta 192.168.15.126 (30 nodos para el tercer departamento).

Cuarta red válida: desde 192.168.15.129 hasta 192.168.15.158.

Quinta red válida: desde 192.168.15.161 hasta 192.168.15.190.

Sexta y última red válida: desde 192.168.15.193 hasta 192.168.15.222.

Como se ve ahora solo podemos aprovechar 6 x 30 = 180 direcciones de las 256 que tenía el rango original de la red de clase C: la pérdida de direcciones IP es el precio que hay que pagar por subdividir la red.

La Fig. 3.23 proporciona un esquema gráfico de la configuración de algunos nodos de cada departamento.

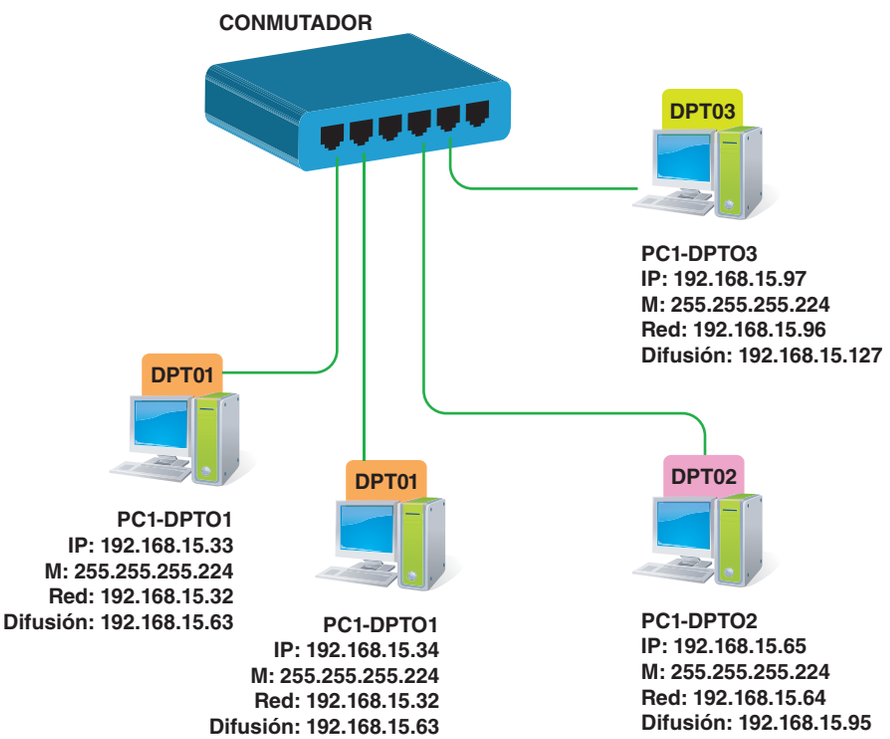
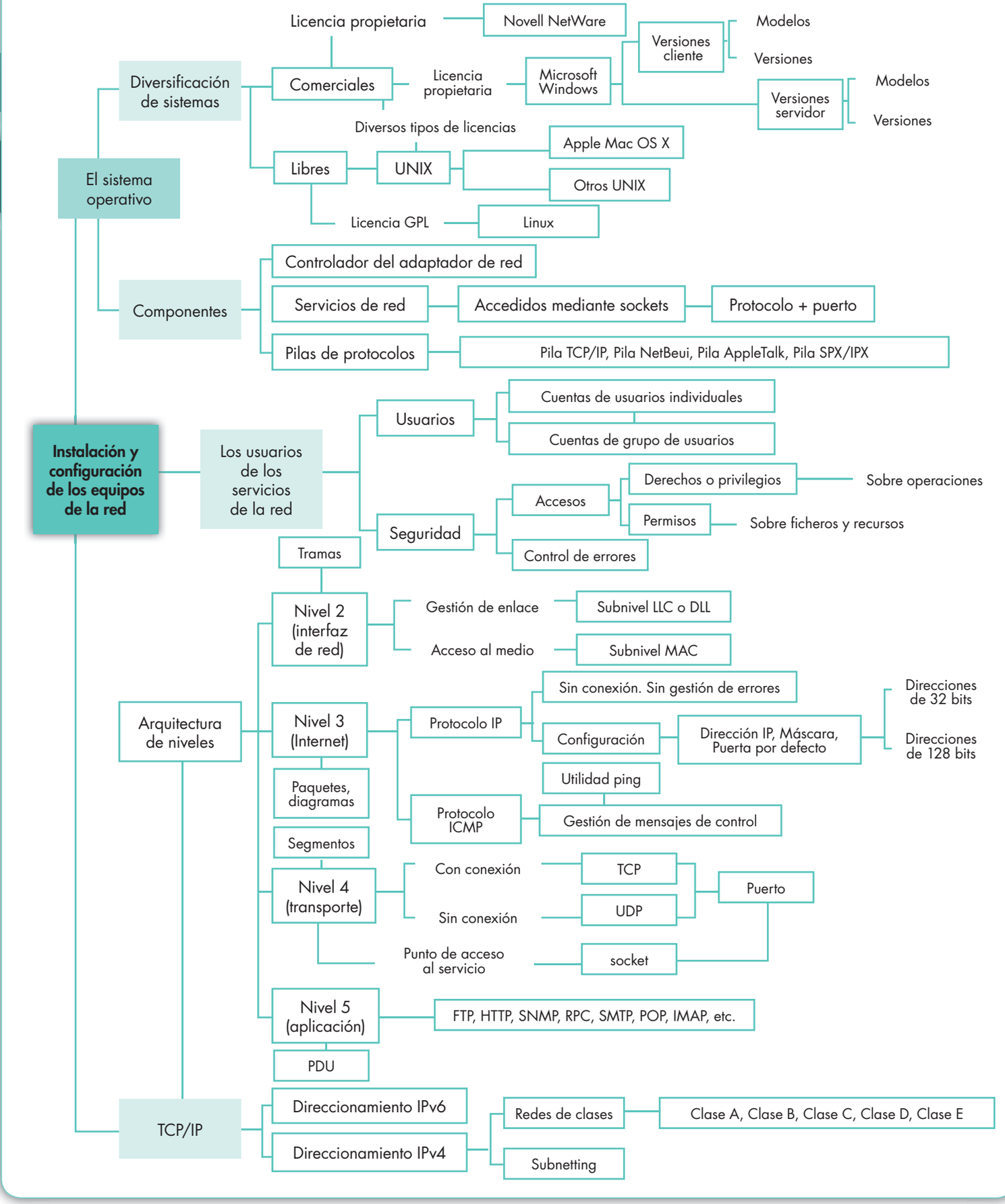


Fig. 3.23. *Parámetros de red de los nodos de cada departamento.*

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de distintos tipos de sistemas operativos de red (hay varias posibilidades en las columnas segunda y tercera):

a) Windows 7	1) Apple	i) Sistema propietario
b) Ubuntu	2) Licencia GPL	ii) Sistema gratuito
c) Fedora	3) Microsoft	iii) NetBeui
d) Mac OS X	4) Linux	iv) TCP/IP
e) Netware	5) Novell	v) SPX/IPX

2. El controlador de una interfaz de red (tarjeta de red) es:

a) hardware.

b) software.

c) firmware.

d) netwware.

3. Asocia los siguientes protocolos a sus equivalentes capas de red en el modelo TCP/IP

a) IP	1) Internet
b) TCP	2) Transporte
c) UDP	3) Aplicación
d) FTP	4) Interfaz de red

4. Un socket es la asociación de:

a) Un protocolo y un número de puerto.

b) Un protocolo y una interfaz de red.

c) Un puerto y una interfaz de red.

d) Dos puertos.

5. Asocia las siguientes direcciones IP con sus correspondientes clases:

a) 10.3.1.15	1) Clase C
b) 130.15.1.4	2) Clase B
c) 195.67.100.5	3) Difusión
d) 224.0.0.30	4) Clase A

6. El protocolo ARP sirve para:

a) Averiguar mediante ping si una máquina remota está activa.

b) Resolver los nombres de las máquinas en sus correspondientes direcciones IP.

c) Resolver las direcciones IP en sus correspondientes direcciones físicas.

d) Comprobar si la tarjeta de red de un equipo funciona correctamente.

7. ¿Cuál es la máscara de red de un nodo cuya red viene especificada por 192.168.15.1/27?

a) 255.255.255.0.

b) 255.255.255.224.

c) 155.155.0.0.

d) 255.255.240.0.

8. Enlaza los siguientes elementos característicos de distintos tipos de protocolos de alto nivel:

a) SMTP	1) Transferencia de ficheros
b) HTTP	2) Diálogo entre aplicaciones
c) FTP	3) Navegación web
d) RPC	4) Intercambio de mensajes de correo

9. Enlaza los siguientes elementos característicos sobre las utilidades básicas de red:

a) ping	1) Gestión de la tabla de direcciones físicas
b) arp	2) Configuración de la red en Windows
c) ipconfig	3) Información sobre el estado de la red
d) iwconfig	4) Gestión de rutas
e) netstat	5) Pruebas sobre el estado activo de las máquinas de la red
f) route	6) Visualización de los saltos que un paquete da en la red hasta llegar a su destino
g) tracert	7) Configuración de la red inalámbrica en GNU/Linux

10. El protocolo ssh cifra las conexiones que realiza para mejorar la seguridad y sustituye a la utilidad más antigua e insegura siguiente:

a) rpc.

b) telnet.

c) tracert.

d) route.

Solución: 1: a-3-(i, iii y iv), b-(2 y 4)-(ii y iv), c-(2 y 4)-(ii y iv), d-1-(i y iv), e-5-(i y v). **2:** b. **3:** a-1, b-2, c-2i, d-3 (no hay ningún protocolo de la capa de interfaz de red). **4:** a. **5:** a-4, b-2, c-1, d-3. **6:** c. **7:** b. **8:** a-4, b-3, c-1, d-2. **9:** a-5, b-1, c-2, d-7, e-3, f-4, g-6. **10:** b.

Comprueba tu aprendizaje

I. Identificar los protocolos y servicios de red disponibles en los sistemas operativos

1. Indica si son verdaderas o falsas las siguientes afirmaciones:
   a) El Unix con marca comercial Mac OS X puede ejecutar AppleTalk como protocolo nativo.
   b) AppleTalk no es compatible con TCP/IP en un sistema Mac OS X.
   c) Microsoft Windows no puede ejecutar TCP/IP.
   d) Linux solo puede ejecutar TCP/IP.
   e) Los sistemas Linux y los sistemas Windows pueden comunicarse a través de TCP/IP.
2. En la tabla siguiente, relaciona los elementos de la izquierda (protocolos) con los de la derecha (servicios).

1. POP	a) Sesión de terminal remoto
2. FTP	b) Discos e impresoras
3. IMAP	c) Intercambio de ficheros
4. SMTP	d) Correo electrónico
5. NetBIOS	
6. Telnet	

3. ¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma red? ¿Por qué?

   ¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma tarjeta de red? ¿Depende de la tarjeta de red o del sistema operativo?
4. Desde las páginas de ayuda de los sistemas operativos Windows y Linux, investiga si ya pueden incorporar la nueva versión del protocolo IP denominada IPv6. Déjate conducir por sus guías de usuario para instalar —en aquellos casos en que se permita— la ampliación del protocolo IPv4 (el que se ha estudiado en esta unidad) con IPv6. También puedes encontrar información a través de los buscadores de Internet por las voces «instalar ipv6» y en la sede web de los fabricantes de sistemas.
5. Prepara unos ordenadores en red que tengan como sistema operativo alguna versión de Windows. Después sigue los siguientes pasos:
   a) Asegúrate de que cada PC tiene un nombre distinto que le identifique unívocamente. Además todos deben pertenecer al mismo grupo o dominio NetBIOS. Tanto el nombre como el grupo al que pertenecen se pueden configurar desde las Propiedades de «Mi PC» (en algunas versiones de Windows, «Mi Equipo»).
   b) No es necesario que estos PC ejecuten el protocolo TCP/IP, basta con que corran NetBeui, pero si tienen TCP/IP asegúrate de que todos comparten el mismo sistema de direccionamiento.
   c) Ahora abre el explorador de Windows y vete desde él a «Mis sitios de red». Investiga en las subcarpetas de la red y verás todos los servicios compartidos a la red que tienen los PC del grupo a través de NetBIOS. Ten en cuenta que solo verás aquellos servicios para los que tengas derecho desde tu cuenta de acceso a la red.

II. Utilizar las herramientas básicas para la gestión de protocolos de red

6. Analiza si son verdaderas o falsas las siguientes afirmaciones:
   a) Una tarjeta de red que tenga instalada la pila TCP/IP no puede instalar la pila SPX/IPX.
   b) Un redirector de red proporciona la interfaz de conexión de servicios a través de varias pilas de protocolos.
   c) NetBIOS no se puede utilizar con TCP/IP, solo puede convivir con protocolos de Microsoft.
   d) Un servicio de disco remoto puede ser alcanzable desde el mismo cliente mediante varios protocolos.
   e) Una impresora remota solo puede admitir conexiones mediante un único protocolo de conexión.
7. Elige un nodo en Internet que tenga respuesta a la orden ping (te puede servir **www.google.com**). Ejecuta ping contra ese nodo y fíjate en el tiempo de respuesta de cada ping realizado. Calcula una media entre todos ellos.

   Ahora ejecuta el ping con el calificador «–l» que acepta como argumento un número entero entre 0 y 65500 que indica el número de bytes que se enviarán con cada orden ping. La orden tendrá el aspecto siguiente: «ping –l 1000 **www.google.com**»

   Ejecuta este ping con 1000, 5000, 10000 y 20000. Mide las medias de todas estas ejecuciones y exprésalas en una gráfica. Observarás cómo a medida que la orden ping genera más tráfico, empezarás a notar una congestión en tu línea de acceso a Internet.
8. Selecciona un grupo de servidores web en Internet. Te puede servir cualquier servidor que puedas localizar en Internet. Ahora ejecuta un comando tracert desde tu PC local hacia esos servidores en Internet. Constata el número de saltos que deben dar los paquetes que envías. Se puede definir una métrica contando el número de saltos hasta alcanzar el destino. Así, por ejemplo, si el tracert a un servidor concreto genera 7 saltos, diremos que el servidor está a una «longitud de red» de 7 saltos del cliente. Ordena ahora los servidores de menor a mayor distancia de red según esa métrica.

Comprueba tu aprendizaje

III. Configurar el sistema de direccionamiento de los equipos de la red

9. Analiza si son verdaderas o falsas las siguientes afirmaciones:

   a) Las direcciones IP son series numéricas binarias de 32 bits.

   b) Todos los ceros y unos de una dirección IP deben estar contiguos.

   c) Todos los ceros y unos de una máscara de red deben estar contiguos.

   d) Los ceros siempre van antes que los unos en una máscara de red.

   e) Hay tres clases de subredes IP.

   f) Un CIDR de /24 es lo mismo que una clase C.

   g) Un CIDR de /24 admite más nodos que un CIDR de /16.

10. Selecciona dos PC en tu laboratorio: uno con sistema operativo Windows y otro con alguna versión de Linux. Realiza ahora las siguientes actividades:

    a) Elige una dirección de red para cada uno de ellos y una máscara de modo que los dos puedan comunicarse en la misma red.

    b) Prueba que tienen comunicación recíproca mediante ping desde uno y otro PC.

    c) ¿Qué utilidades puedes utilizar para comprobar que se comunican entre sí?

    d) Ejecuta un tracert desde uno al otro. ¿Cuántos saltos ves en el tracert realizado?

11. Toma dos PC con sistema operativo Linux y Windows respectivamente. Asegúrate de que el PC Linux tiene instalado un servidor Telnet o al menos puede aceptar conexiones interactivas remotas de terminal. Ahora ejecuta las siguientes acciones:

    a) Examina los dos PC y apunta las direcciones IP de cada uno de ellos. Asegúrate de que están en la misma red IP para que puedan tener comunicación entre ellos.

    b) Ejecuta desde el PC Windows un Telnet hacia el PC Linux. Si tienes Windows Vista tendrás que instalar previamente un cliente Telnet equivalente (puede servirte PuTTY). Comprueba que puedes crear sesiones remotas.

    c) Crea algunos ficheros en el PC Linux utilizando esa sesión remota y luego comprueba desde la consola local del PC Linux que efectivamente se crearon.

    d) Ejecuta el comando de apagado del sistema Linux desde la consola remota en el PC Windows. Observarás que el PC Linux se apaga. ¿Qué ocurre con la conexión Telnet? ¿Por qué? ¿Puedes encender remotamente el PC Linux desde el PC Windows?

12. Una empresa quiere fraccionar su sistema de direccionamiento de red en cinco subredes. La dirección de red de la que se parte es 192.168.3.0/24.

    a) ¿Cuáles son los parámetros de red que hay que configurar en el tercer PC de la primera subred válida?

    b) ¿Cuál es la dirección de difusión de la tercera subred válida?

    c) ¿Cuál es la dirección de red de la segunda subred válida?

Unidad 4

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

SMR_RL_AAbad_04_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

Ampliación

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.

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.

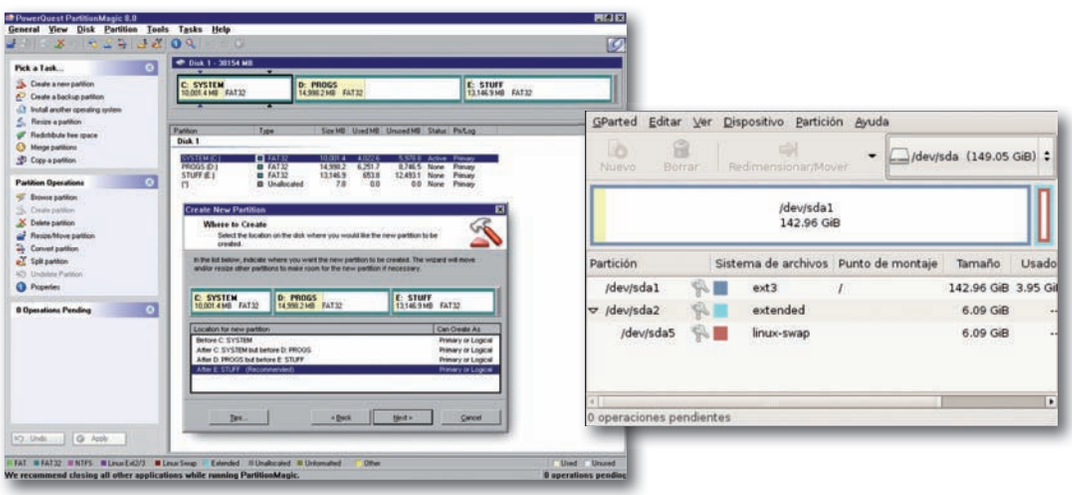


Fig. 4.1. *Consola de una conocida marca de programa gestor de particiones de volúmenes para Windows (a la izquierda). Su equivalente de software libre, GParted, sobre Linux (a la derecha).*

CEO

SMR_RL_AAbad_04_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, podremos compartir cualquier otra carpeta.

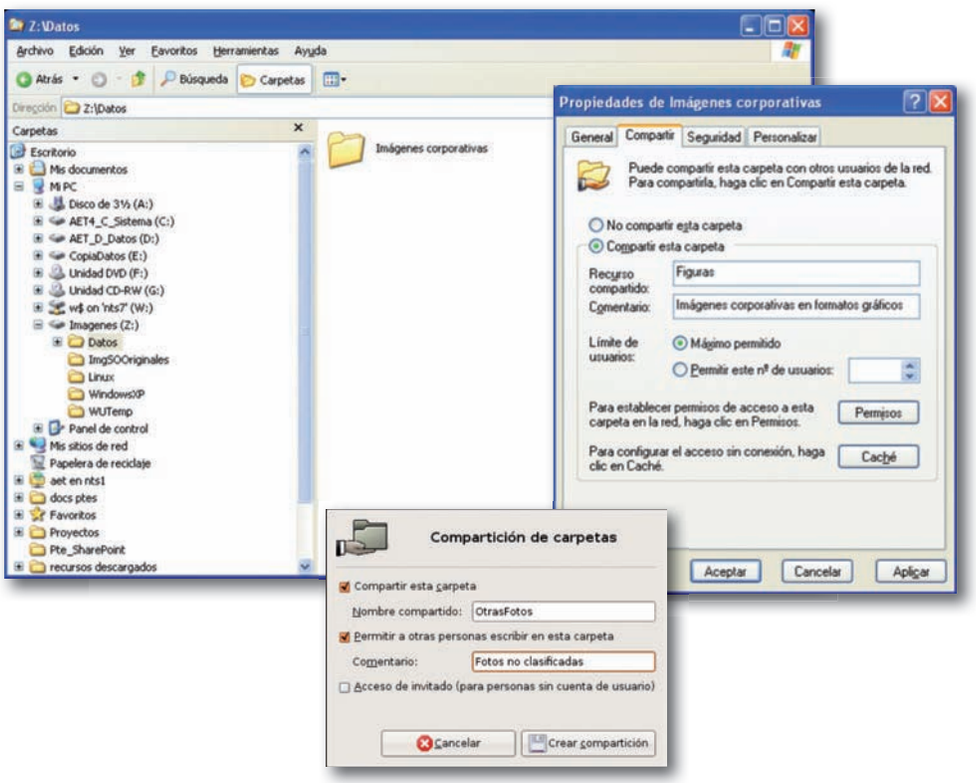


Fig. 4.2. *Uso compartido de carpetas en Windows (arriba) y en Linux (abajo).*

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».

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

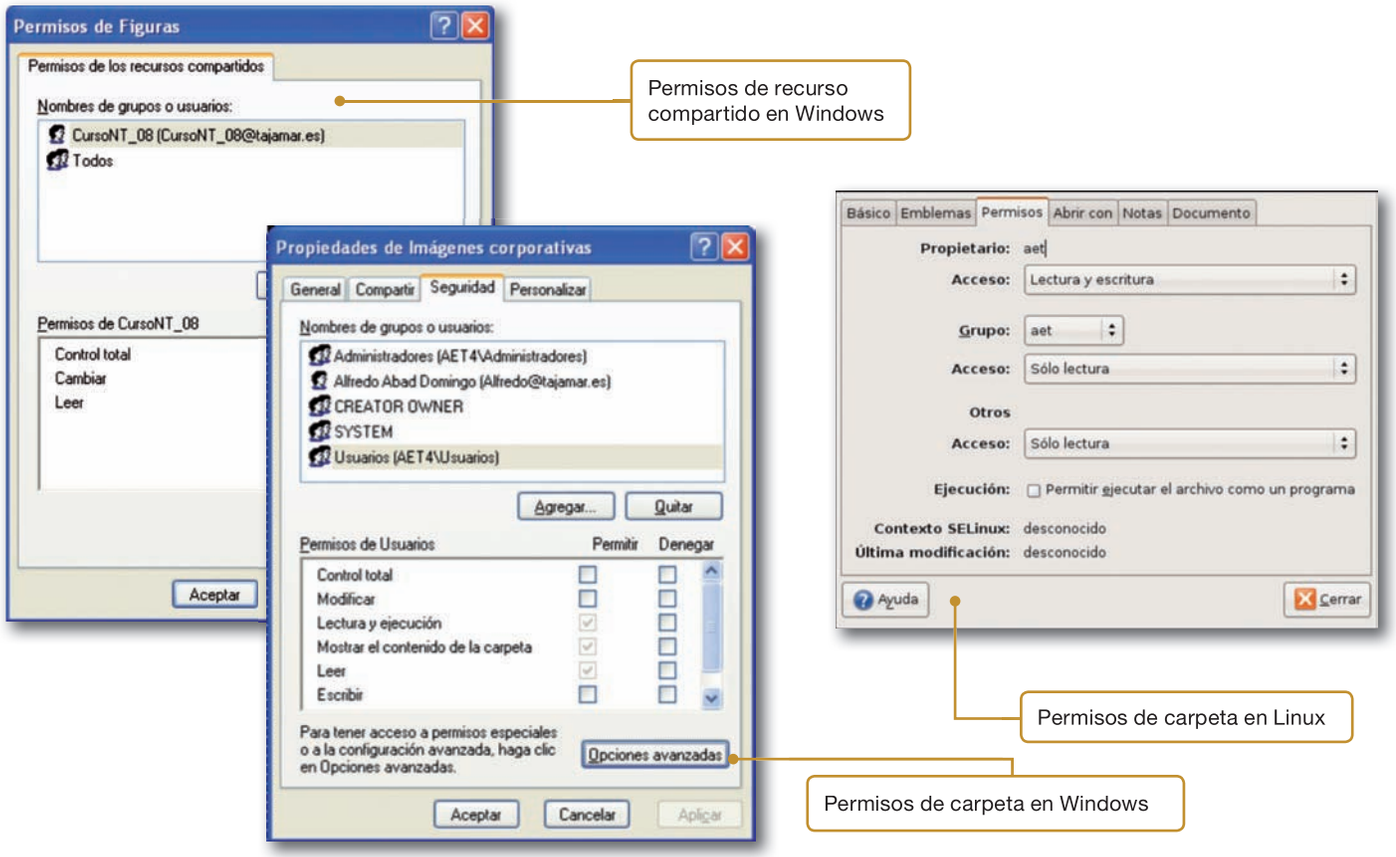


Fig. 4.3. *Ficha de permisos de recursos y carpetas en Windows (a la izquierda) y de carpeta en Linux (a la derecha).*

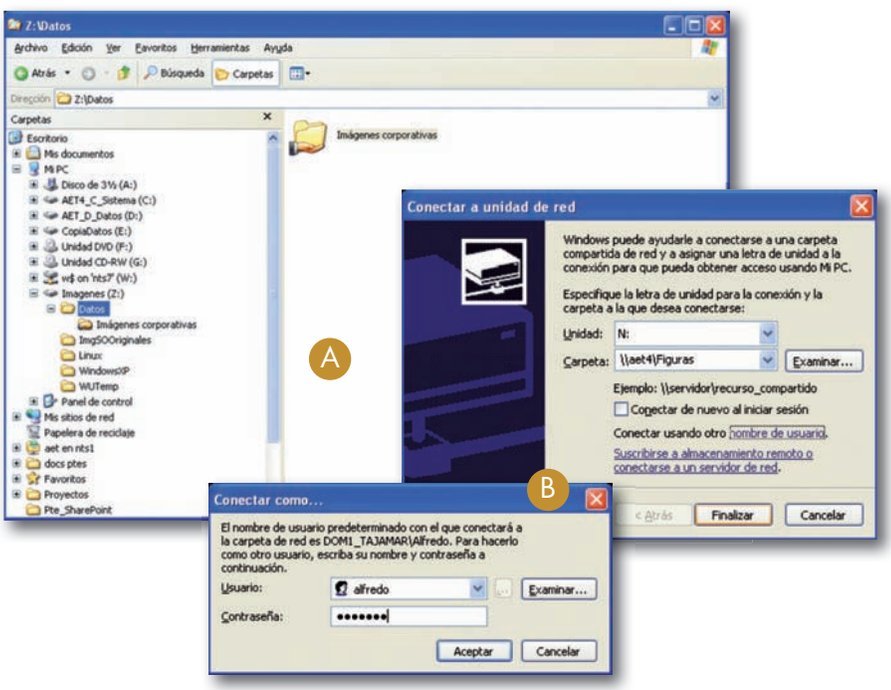


Fig. 4.4. *A) Aspecto para el sistema operativo servidor de una carpeta compartida. B) Fichas de conexión a la carpeta compartida desde un cliente de red.*

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.

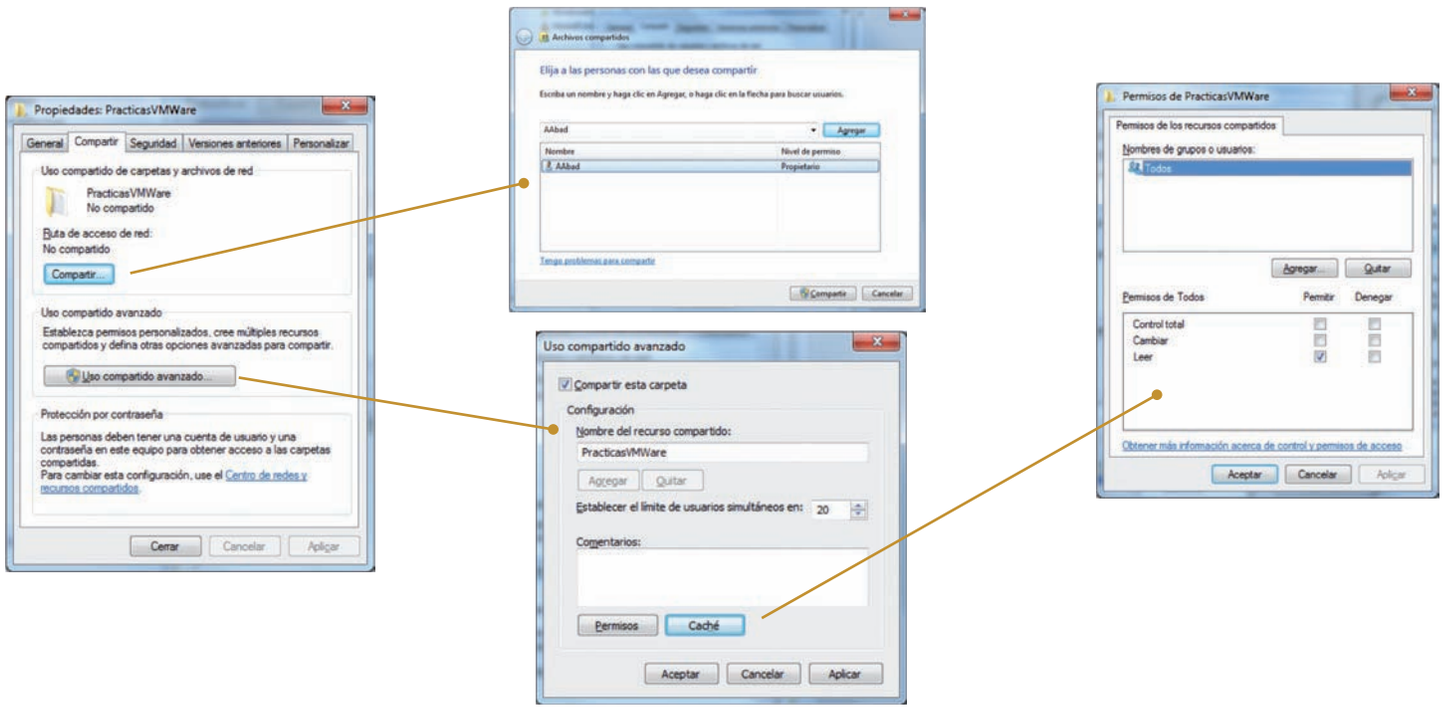


Fig. 4.5. *Vista de la configuración del proceso de compartir carpetas en Windows 7.*

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 redunda en una mayor eficacia del sistema así como en un abaratamiento de los costes de instalación al poder reducir el número de impresoras sin perder funcionalidad.

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

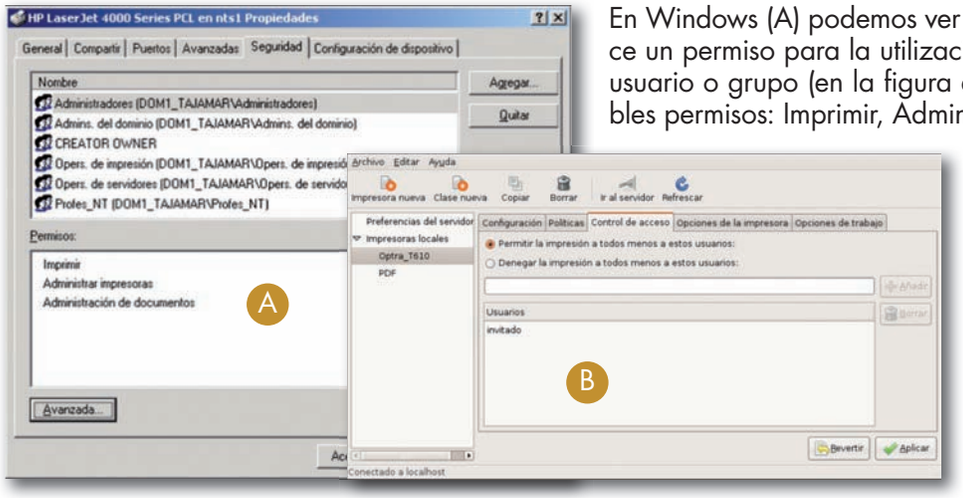
SMR_RL_AAbad_04_ImpresorasRedFax.docx

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.



En Windows (A) podemos ver los usuarios y grupos sobre los que se establece un permiso para la utilización de la impresora. Una vez seleccionado un usuario o grupo (en la figura el grupo de Administradores), caben tres posibles permisos: Imprimir, 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.

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

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.

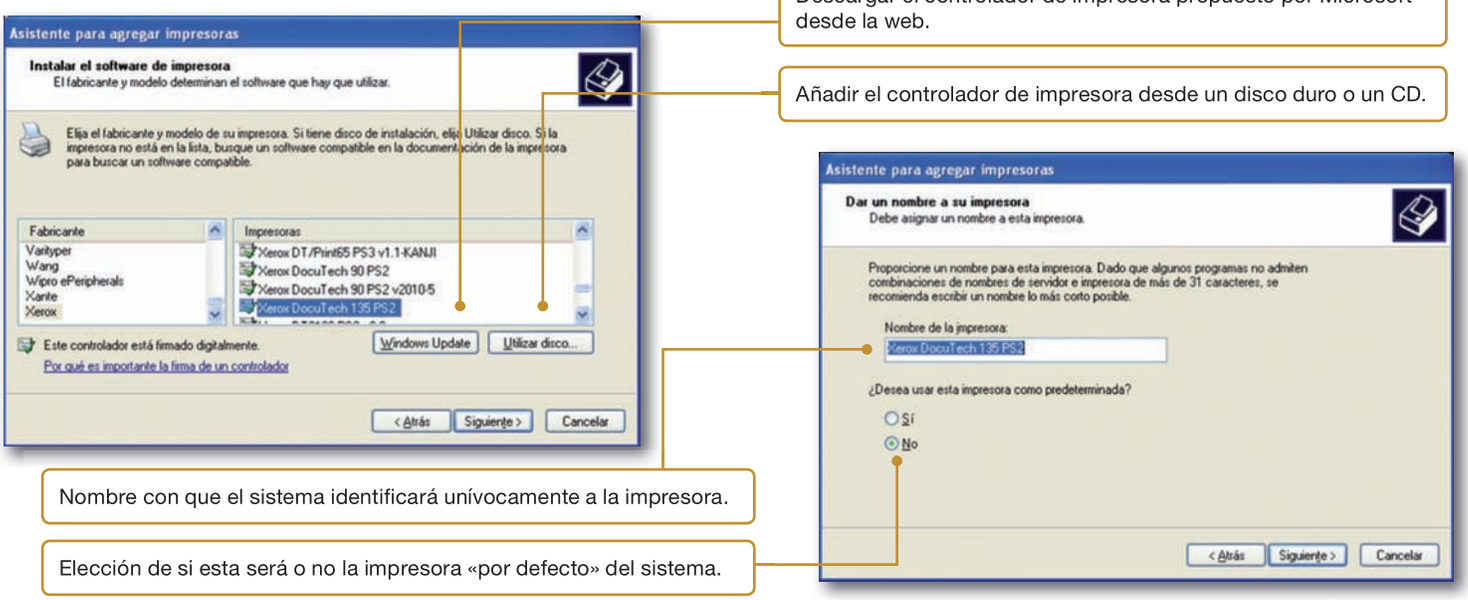


Fig. 4.7. *Ventanas de selección del controlador de impresora (A) y asignación del nombre de la impresora (B).*

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 nombre 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.

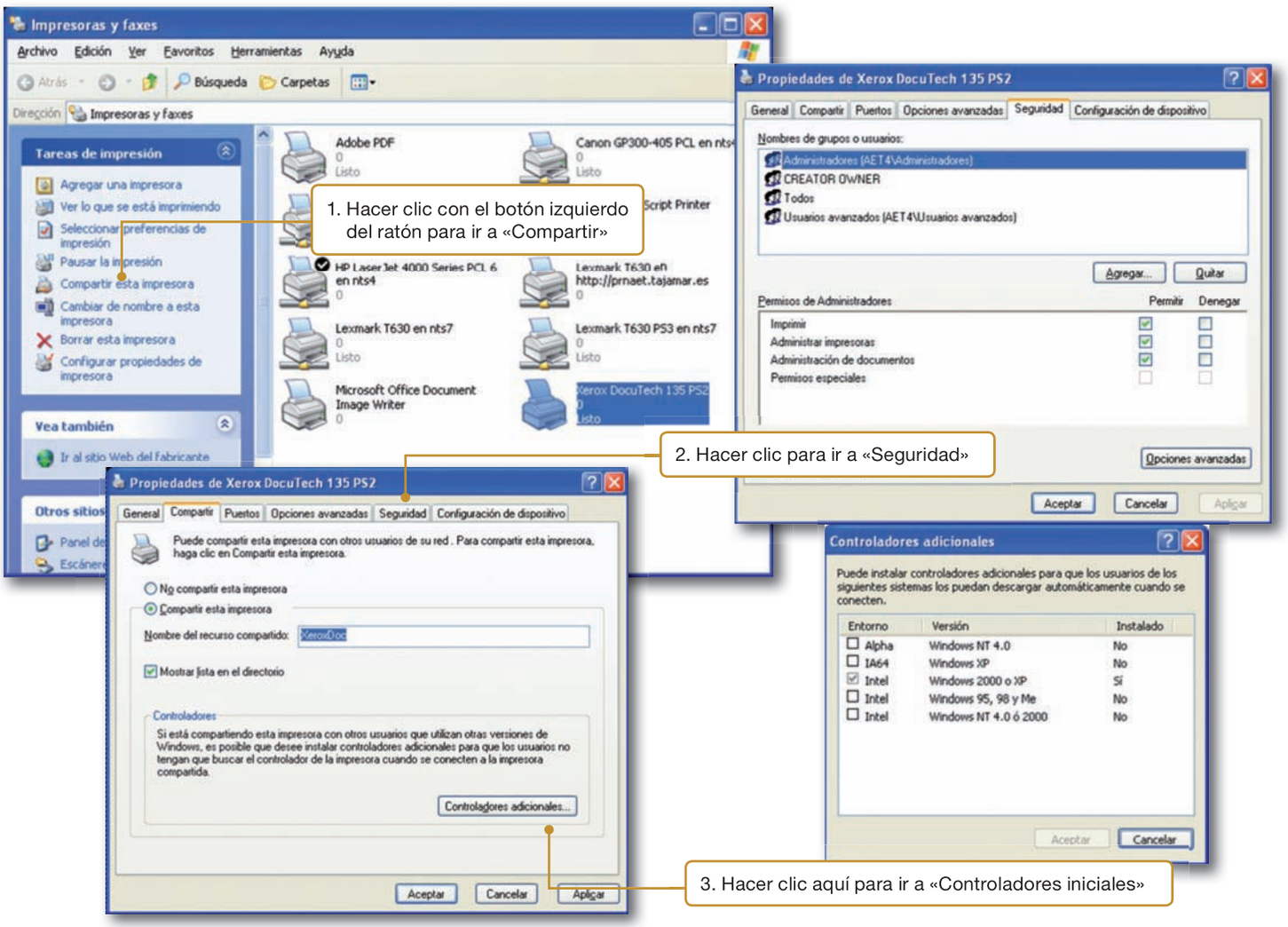


Fig. 4.8. *Ventanas de creación de un recurso de impresión compartido, seguridad y controladores adicionales.*

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 tendremos 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).

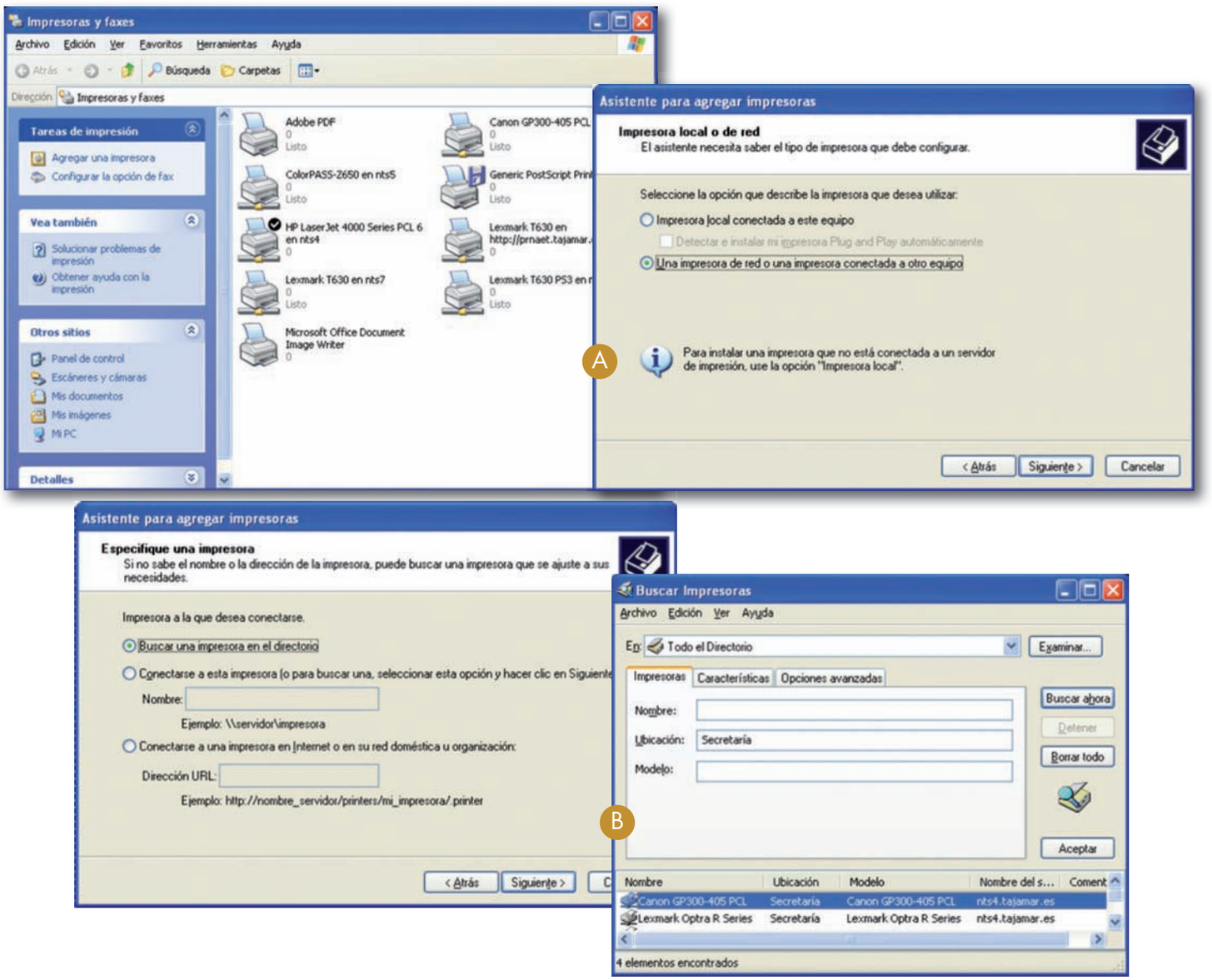


Fig. 4.9. *A) Conexión a una impresora de red. B) Búsqueda de una impresora en el Directorio Activo.*

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.

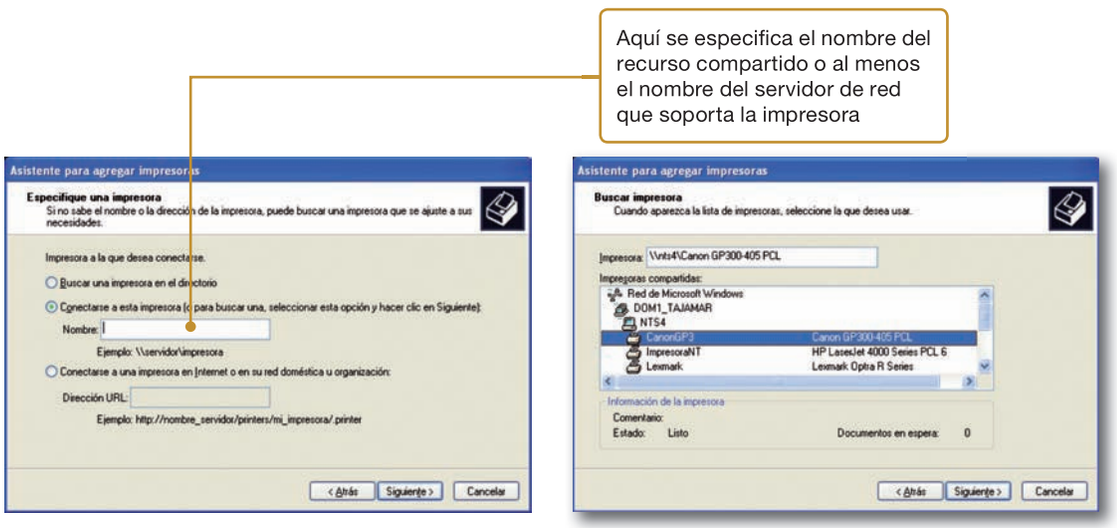


Fig. 4.10. *Búsqueda de una impresora en toda la red sin utilizar el Directorio Activo.*

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).

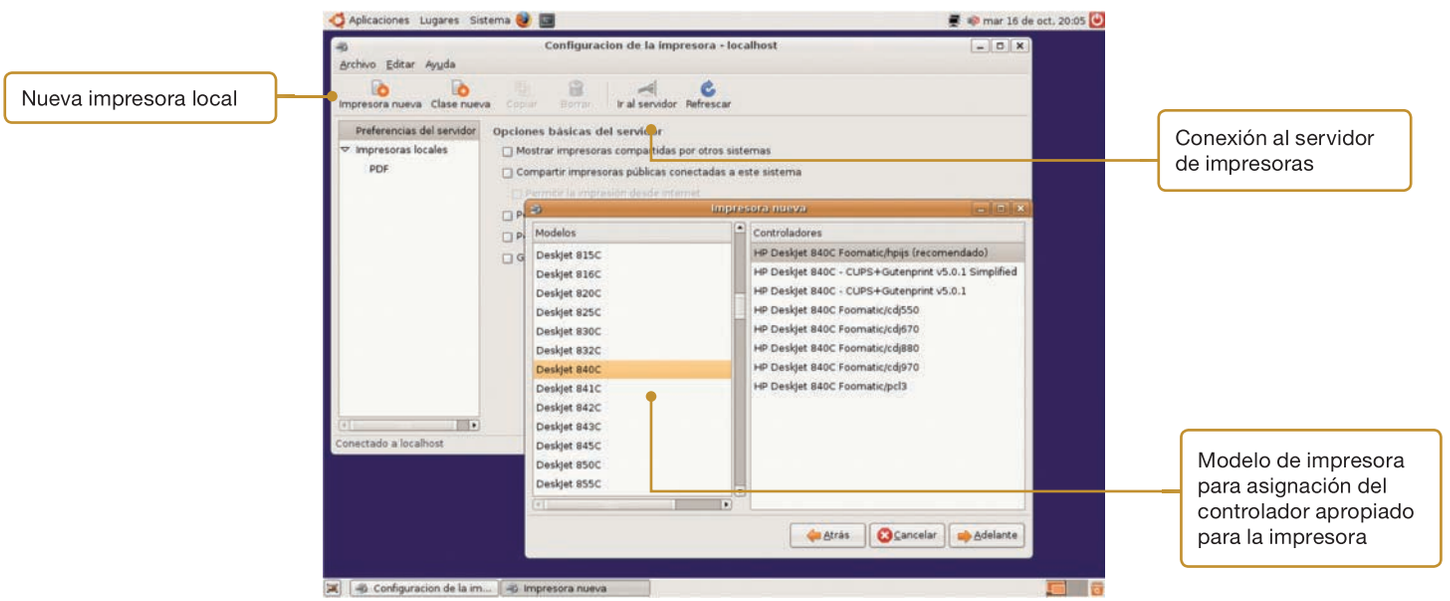


Fig. 4.11. *Configuración de impresoras locales o remotas en Linux.*

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. Asígnale 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.

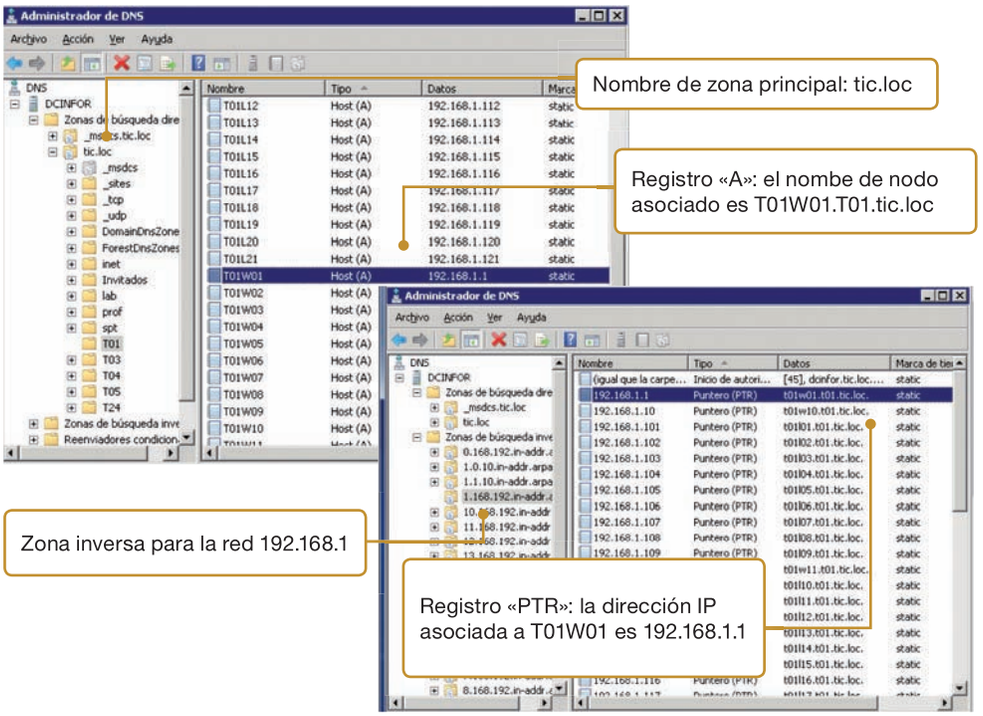


Fig. 4.12. *Representación gráfica de un servidor DNS sobre un servidor Windows Server 2008 R2: zona directa (izquierda) y zona inversa (derecha).*

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.

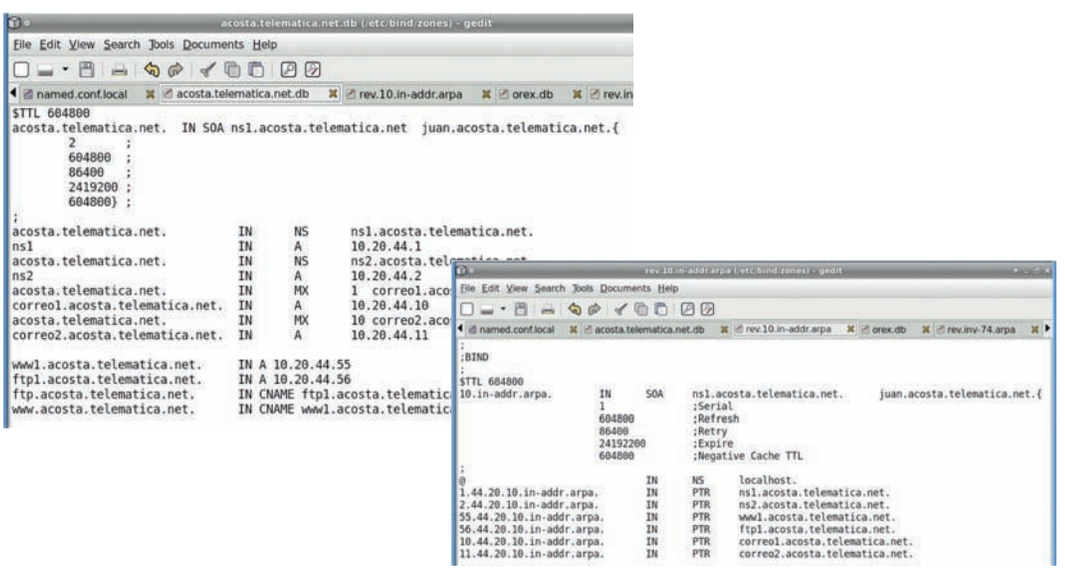


Fig. 4.13. *Vista del fichero de configuración en bind9 de una zona DNS directa (izquierda) y otra inversa (derecha).*

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 predeterminado 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.

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.

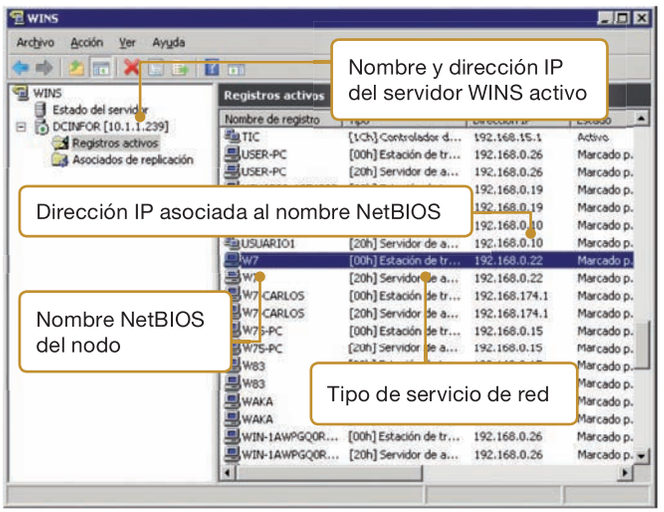


Fig. 4.14. *Consola de administración de un servidor WINS sobre Windows Server 2008 R2.*

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.

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.

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: **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. 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.

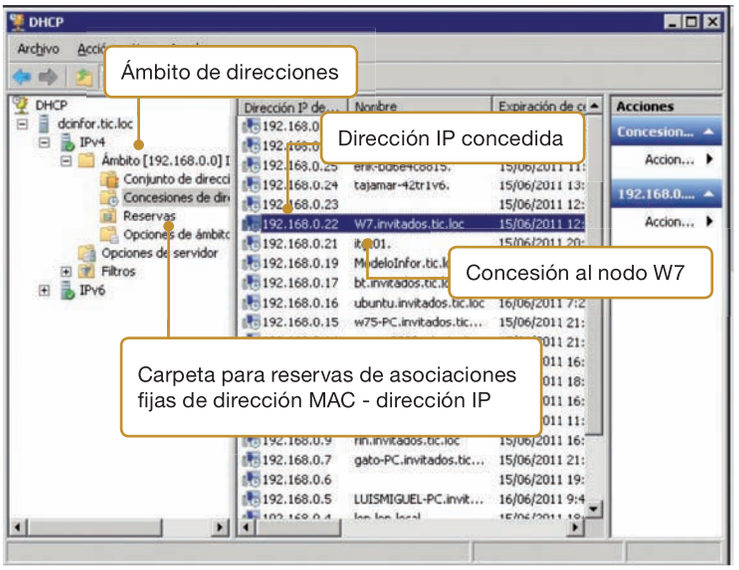


Fig. 4.15. *Representación gráfica de un servidor DHCP sobre Windows Server 2008 R2.*

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 enrutadores 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 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 resolvedor 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 resuelves 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

SMR_RL_AAbad_04_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.

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.

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.

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.

CEO

SMR_RL_AAbad_04_ConfigMailMarshal.docx

Documento que contiene información sobre configuración de un servidor de correo electrónico (MailMarshal).

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.

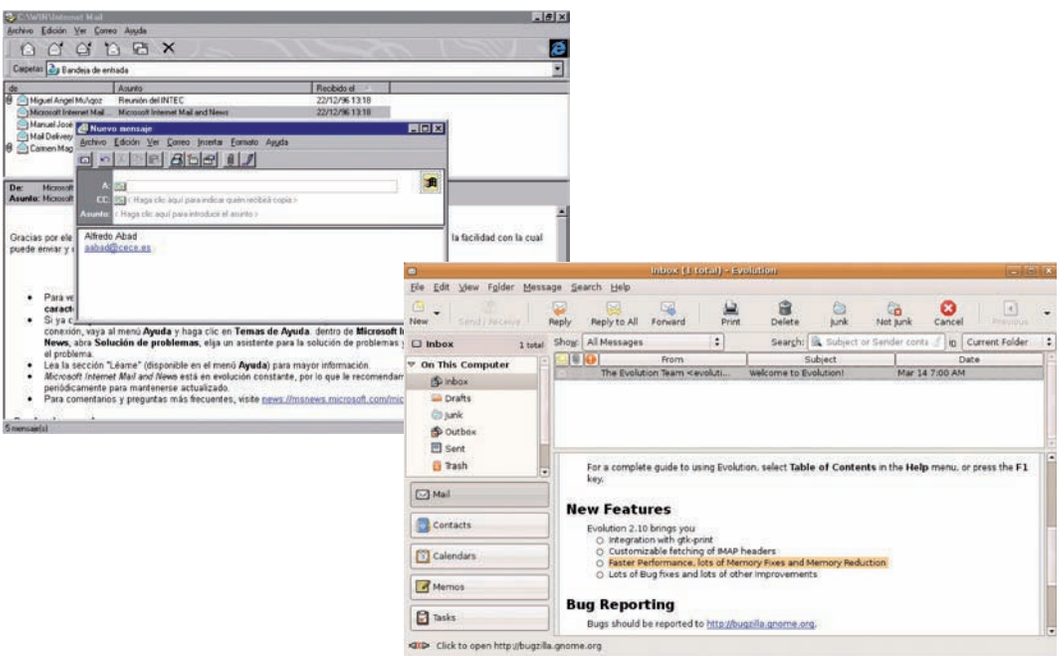


Fig. 4.17. *Cliente de correo electrónico para Internet y confección de un nuevo mensaje con Outlook Express (izquierda) y cliente de correo electrónico de software libre (Evolution) para Linux (derecha).*

CEO

SMR_RL_AAbad_04_CorreoSpam.docx

Documento que contiene información sobre correo spam no deseado.

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.

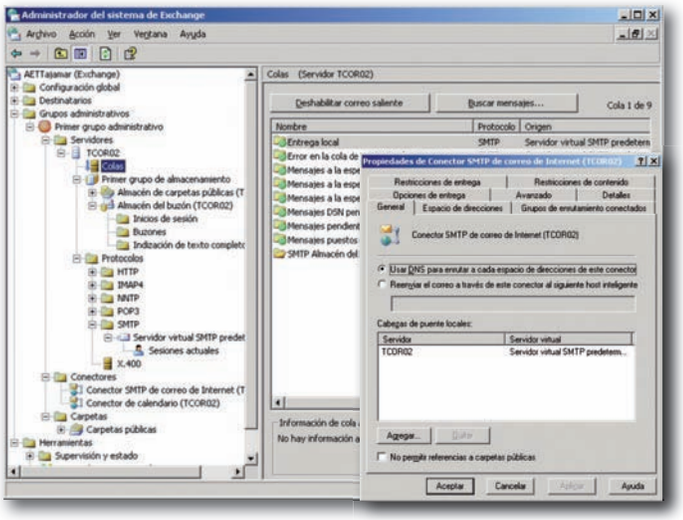


Fig. 4.18. *Consola de administración de Microsoft Exchange Server.*

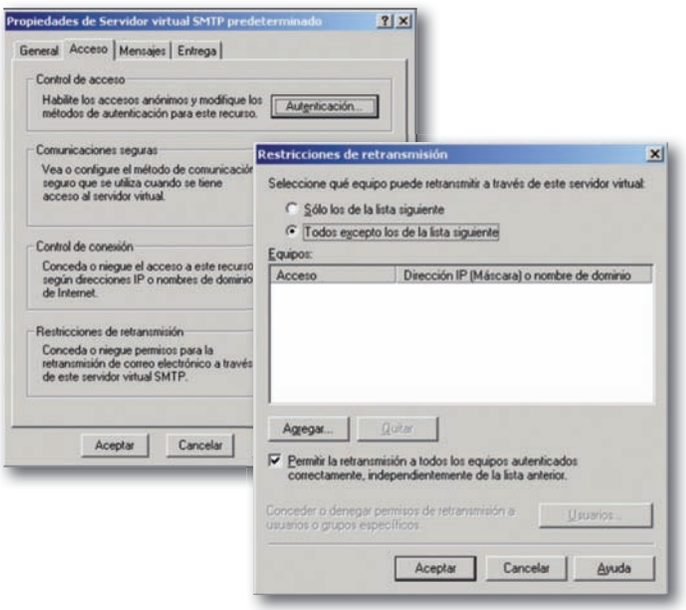


Fig. 4.19. *Algunos detalles de las fichas de configuración del servidor SMTP para Microsoft Exchange Server, el servidor de correo electrónico empresarial de Microsoft.*

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 indeseadamente 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.marshal.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. Después abre una sesión en diversos clientes Windows y Linux y comprueba que pueden enviar y recibir correo electrónico.

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 conmutadores 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.

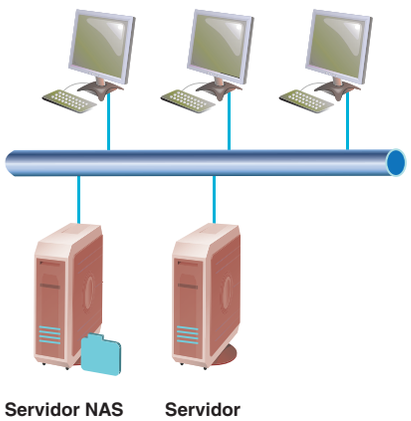


Fig. 4.20. *Almacenamiento NAS.*

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.

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).

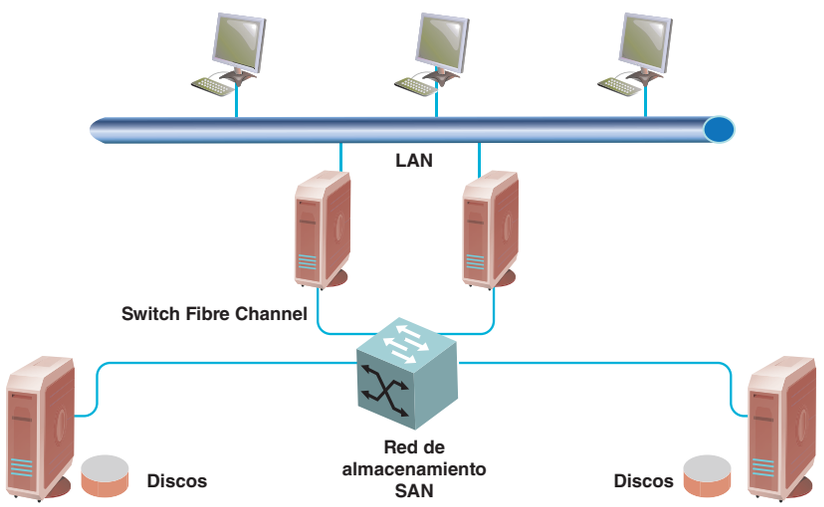


Fig. 4.21. *Modelo de almacenamiento SAN.*

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.

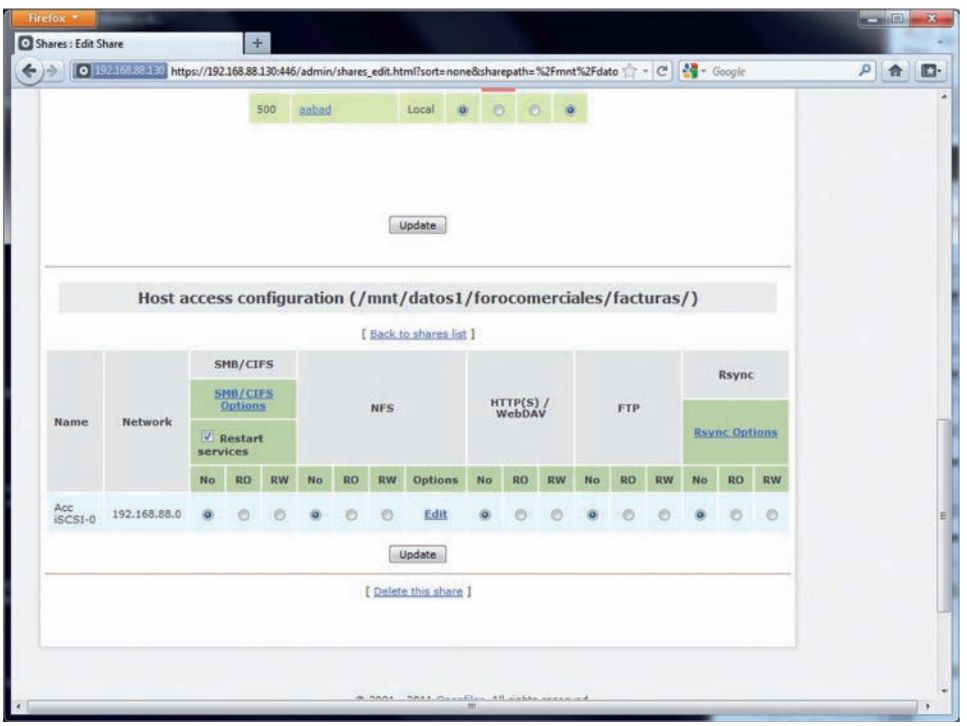


Fig. 4.22. *Página web de gestión de las unidades de red compartidas bajo diversos protocolos en Openfiler, una distribución Linux que gestiona servicios de disco mediante SMB/CIFS, NFS y otros protocolos de red.*

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.

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.

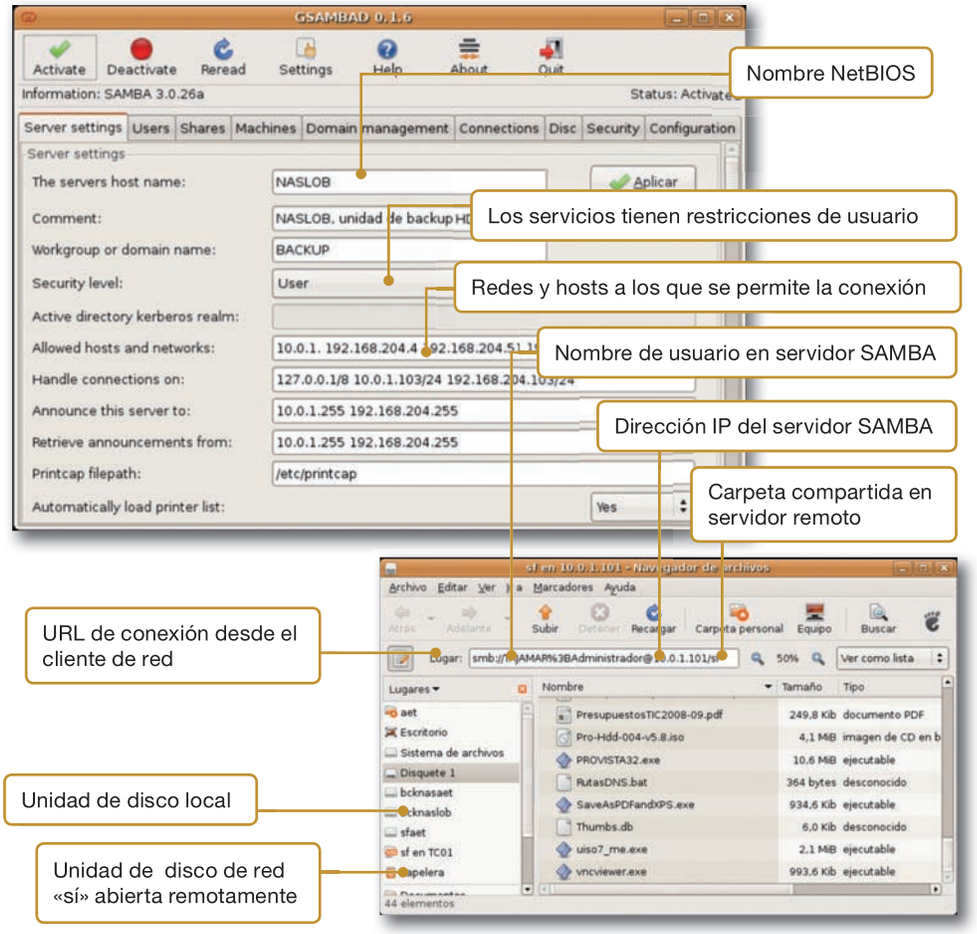


Fig. 4.23. *Consola de configuración de un servidor Samba sobre Linux (a la izquierda) y apertura de una unidad de red Windows mediante un cliente Samba de Linux (a la derecha).*

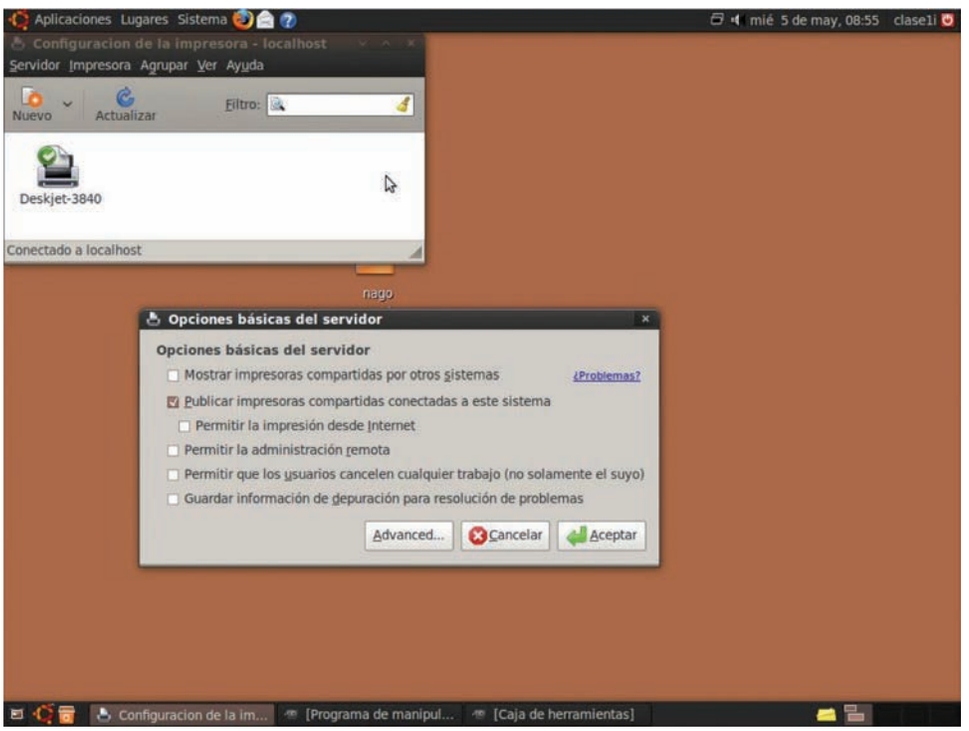
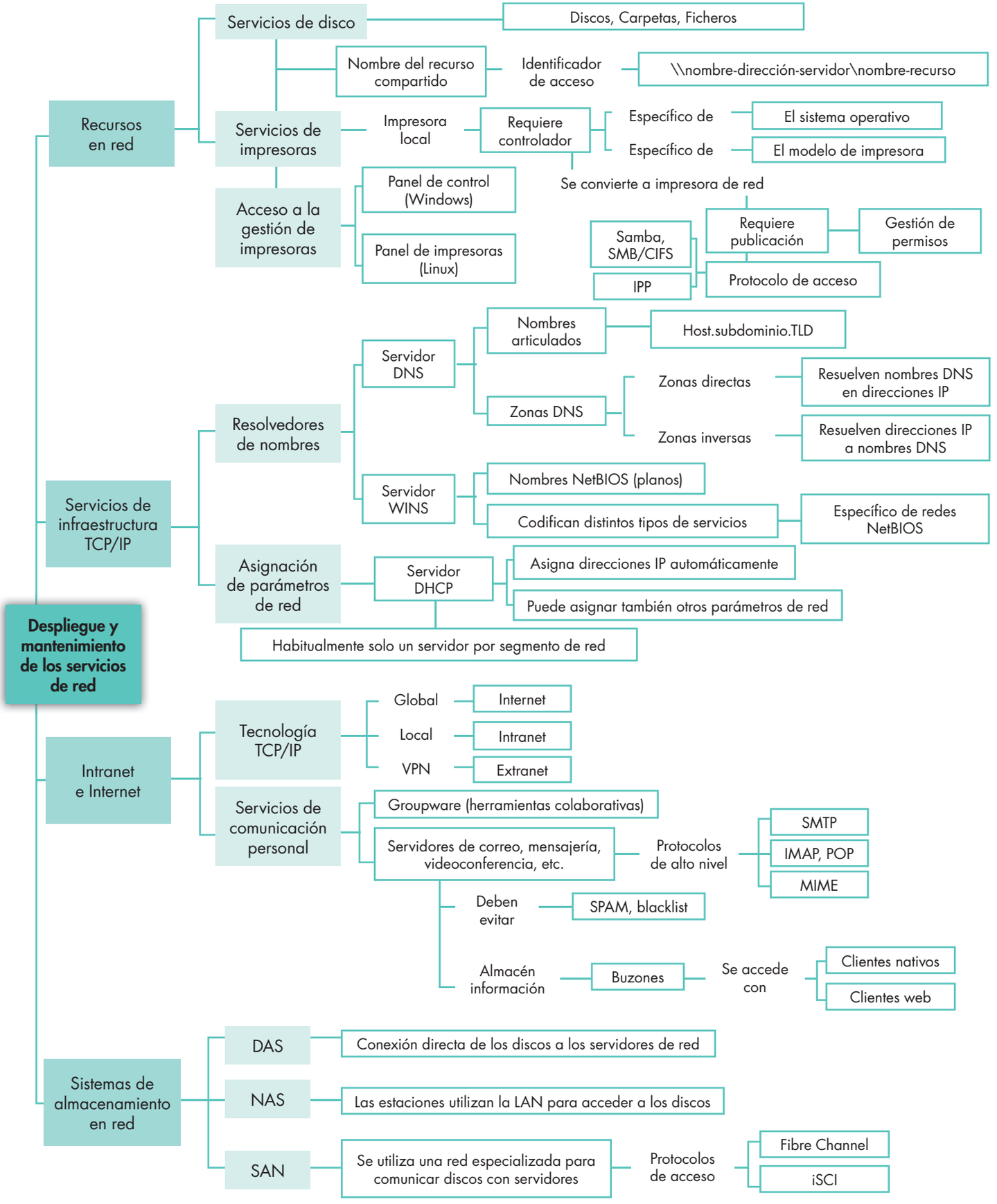


Fig. 4.24. *Publicación de una impresora local en una estación Ubuntu mediante Samba.*

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, denegándoselo 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 DCHP 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	
Regitro 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.

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).

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, conmutadores, punto de acceso y videocámara) tienen direcciones 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 dispondremos 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 desempaqueta 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).

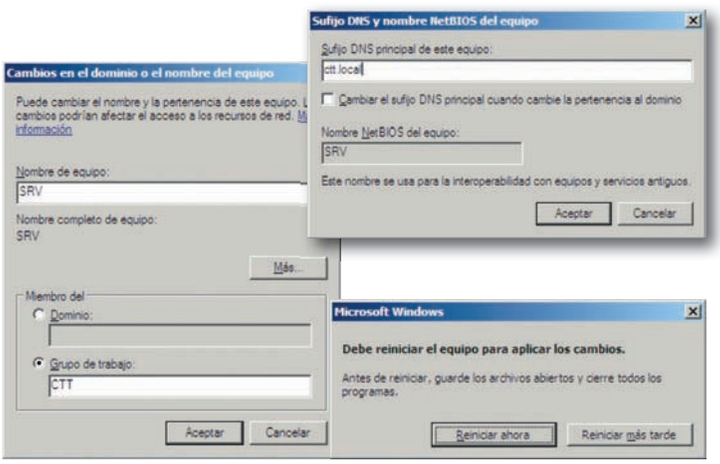


Fig. 1. *Configuración del nombre del equipo, grupo de trabajo y dominio DNS.*

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

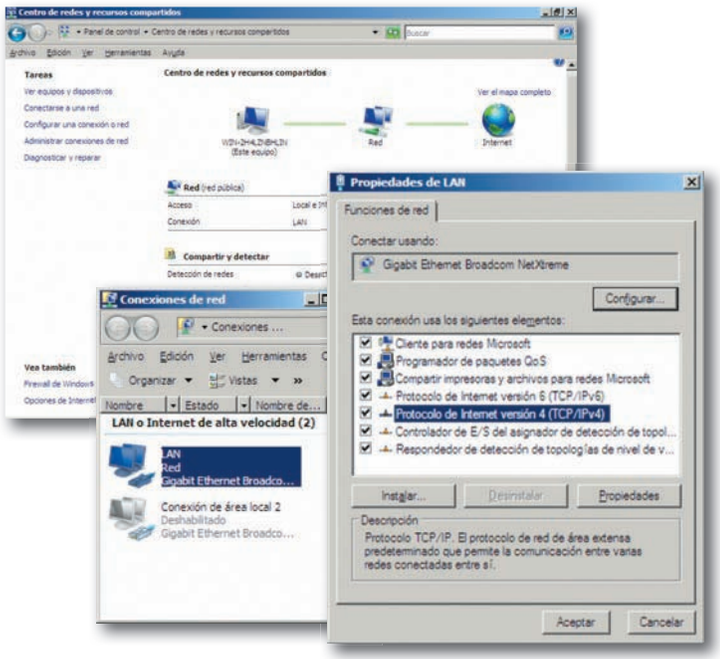


Fig. 2. *Configuración de la red en la interfaz LAN.*

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).

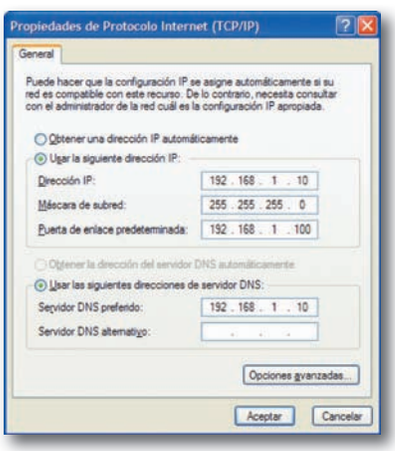


Fig. 3. *Configuración de los parámetros IPv4 en la interfaz de red LAN.*

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 aceptamos 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).

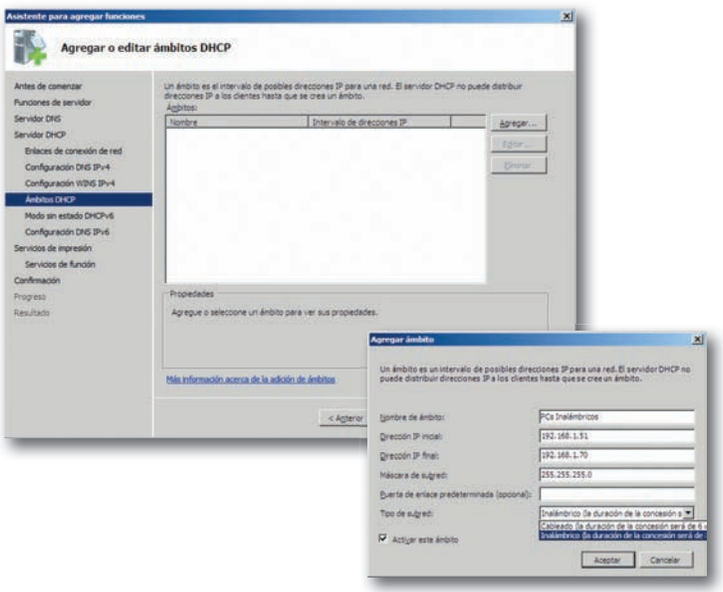


Fig. 4. *Creación de un ámbito DHCP.*

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 *ctt.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).

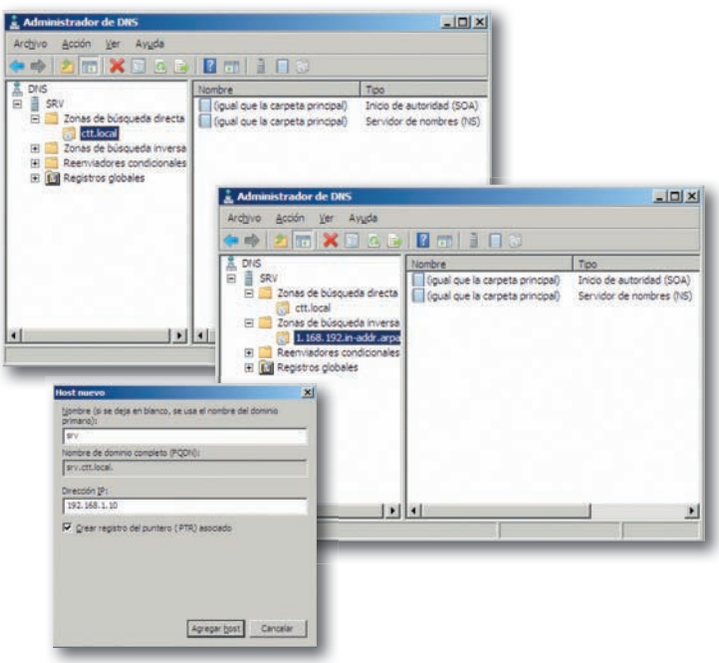


Fig. 5. *Zona directa, zona inversa y alta de un nodo en el servicio DNS.*

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

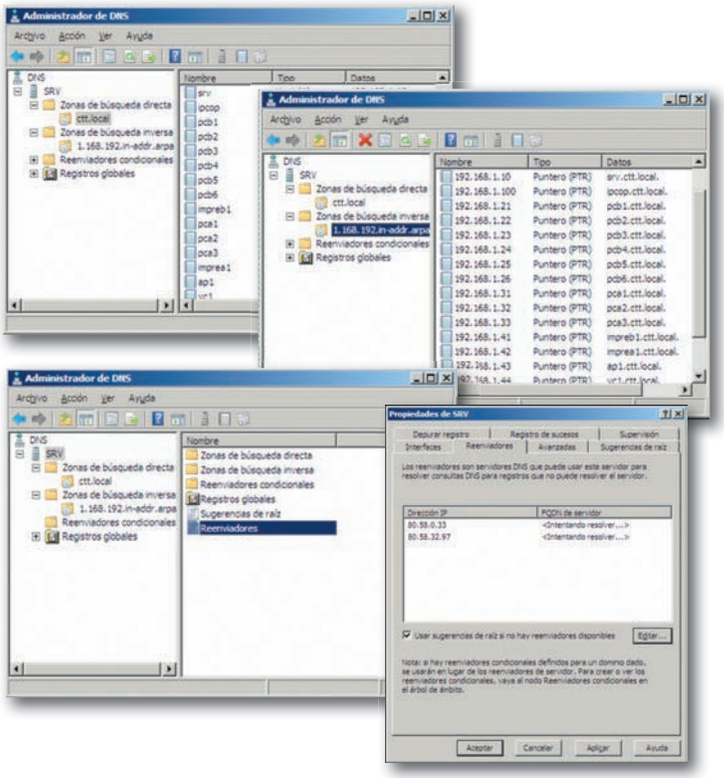


Fig. 6. *Zona directa e inversa con los nodos de la LAN (arriba). Configuración de los reenviadores en el servicio DNS (abajo).*

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 *ctt.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 icono 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).

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.

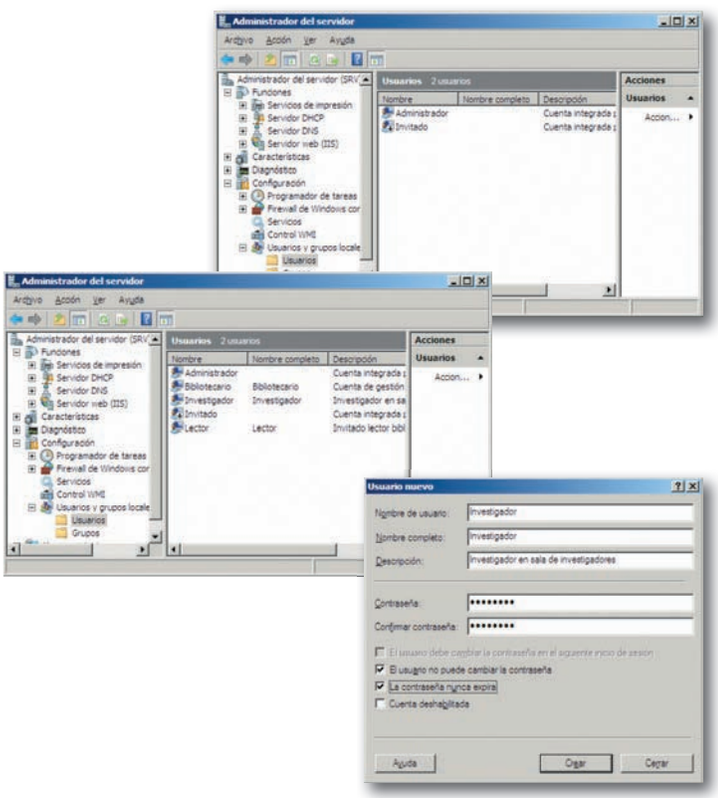


Fig. 7. *Consola de administración de usuarios antes y después de la creación del usuario Investigador.*

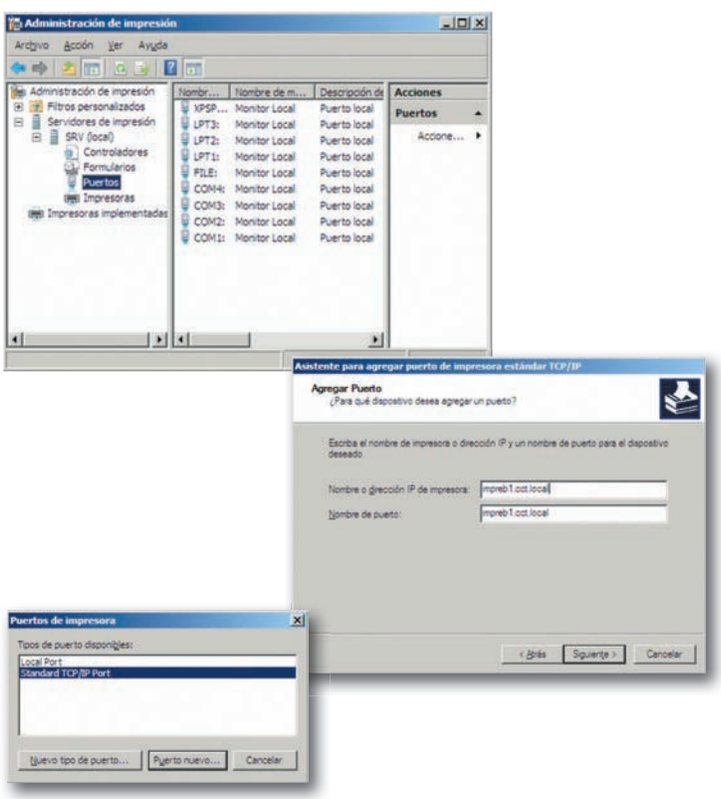


Fig. 8. *Alta de un puerto de red para una impresora de red.*

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 compartirla 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).

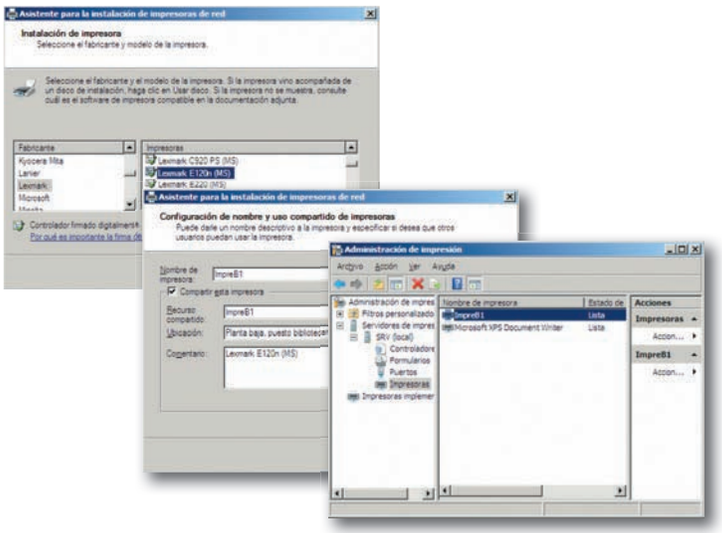


Fig. 9. *Elección del controlador de la impresora, compartición en red y vista de la consola de administración con la nueva impresora creada y compartida.*

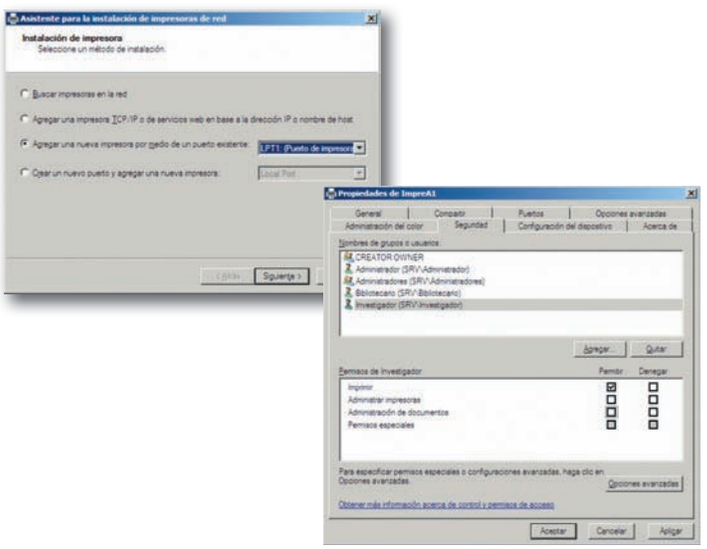


Fig. 10. *Elección de un puerto local (LPT1) para una impresora local servida en la red (a la izquierda) y asignación de permisos de impresión para una impresora (a la derecha).*

Práctica final

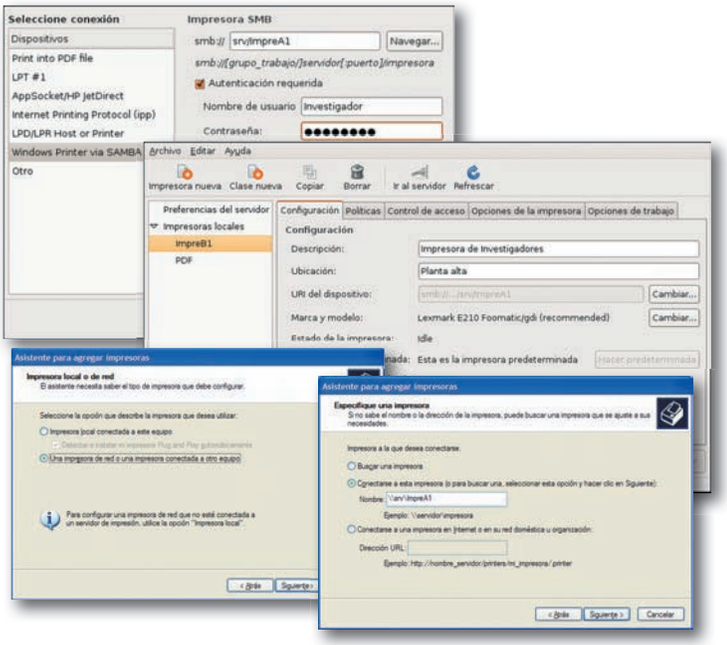


Fig. 11. *Secuencia de conexión a una cola de impresora remota desde una estación cliente Linux (arriba) y Windows (abajo).*

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_CarpetasRed.pptx

Documento que contiene información sobre configuración de carpetas compartidas en la red.

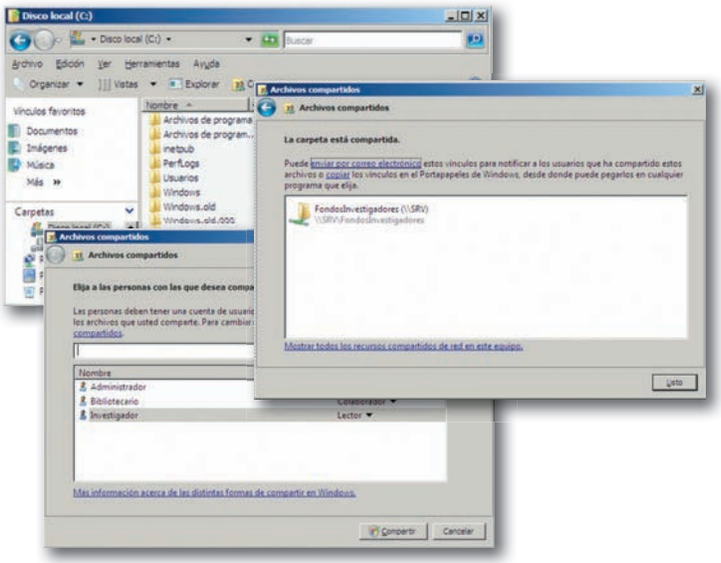


Fig. 12. *Pasos para compartir una carpeta a la red.*

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).

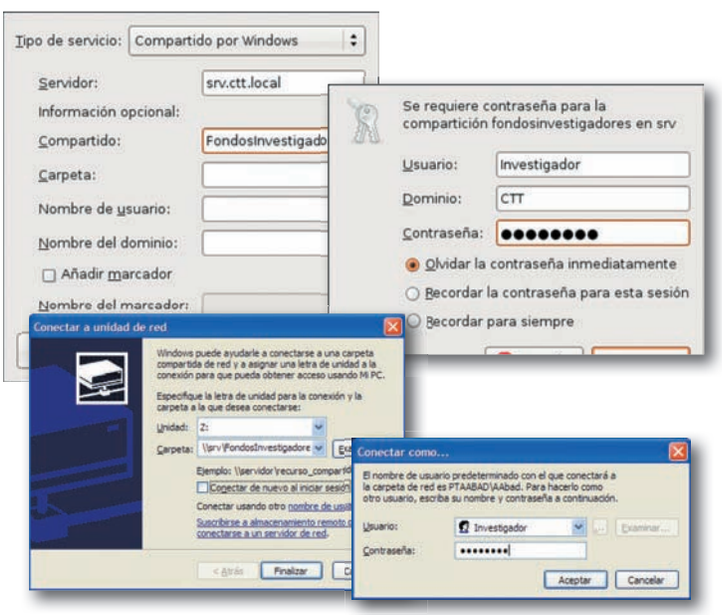


Fig. 13. *Secuencia de conexión a una carpeta de red desde un cliente Linux (arriba) y Windows (abajo).*

Unidad 5

Dispositivos específicos de la red local

En esta unidad aprenderemos a:

- Distinguir las funciones de los dispositivos de interconexión de la red.
- Elegir los dispositivos de red de área local en función de las necesidades.
- Configurar redes locales virtuales y gestionar los bucles de la red.

Y estudiaremos:

- El funcionamiento del módem.
- La funcionalidad de *hubs* y conmutadores.
- El comportamiento de los sistemas operativos en la configuración de redes.

CEO

SMR_RL_AAbad_05_ModemsAnalogicos.docx

1. Elementos del módem analógico.
2. Normativas estándares para módems y lenguaje Hayes.
3. Caso práctico de utilización de Hyperterminal.

Claves y consejos

En ADSL hay que distinguir el ancho de banda de subida del de bajada, es decir, la velocidad a la que se pueden poner datos en la red y a la que se pueden descargar es diferente, lo que hay que tener en cuenta si hay mucho tráfico de salida hacia Internet ya que la velocidad de subida es mucho menor que la de bajada.

Truco

En las instalaciones domésticas en las que se comparten varios supletorios telefónicos sobre la misma línea compartida con el servicio ADSL, debe instalarse en cada teléfono un microfiltro que filtra la señal de voz hacia el teléfono impidiendo que le llegue la señal de modulación de ADSL, que se interpretaría en el teléfono como ruido.

CEO

SMR_RL_AAbad_05_AccesoInternetModem.docx

Documento sobre:

1. Cómo acceder a Internet mediante módem analógico.
2. Comprobación y configuración del módem.

1. El acceso remoto a la red

Una vez concluido el estudio del nivel físico de la red —cables, conectores e instalación a lo largo de la edificación—, hay que analizar los dispositivos que permiten el intercambio de datos entre los diferentes nodos de la red, incluso aunque estén situados en distintos segmentos de la misma.

Además, nos adentraremos en la creación de redes de área local virtuales, que permiten corregir la inflexibilidad del sistema de cableado, al igual que la conexión de un nodo a un segmento de red con independencia de su ubicación física.

El acceso a los servicios proporcionados por la red de área local se realiza normalmente desde las estaciones conectadas a la misma LAN. Sin embargo, en ocasiones esto no es posible debido a la distancia geográfica que separa al cliente del servidor.

Vamos a estudiar algunas de las tecnologías utilizadas para conseguir un acceso remoto. Tradicionalmente se han utilizado módems analógicos, pero con la llegada de la banda ancha, esto ha sido sustituido por módems ADSL o de cable u otras tecnologías de alta velocidad.

1.1. El módem ADSL y el cable-módem

Estrictamente hablando, el módem es un conversor analógico-digital que se utiliza para transmitir información digital por las líneas telefónicas apropiadas para la transmisión de señales analógicas. Sin embargo, también suele aplicarse este término para el caso de los módems ADSL o los módems de cable.

A. Tecnología ADSL

DSL son las siglas de *Digital Subscriber Line*. Delante de estas siglas suele ponerse otra letra que identifica la familia específica dentro de DSL, por ello nos referiremos, en general, a tecnologías xDSL.

Con ADSL se trata de aprovechar el mismo cableado del teléfono analógico para la transmisión de datos a Internet a alta velocidad estableciendo dos canales de comunicación sobre la misma línea física.

De todas las modalidades de DSL, nos centraremos básicamente en ADSL por ser la tecnología mayoritariamente implantada por las compañías telefónicas.

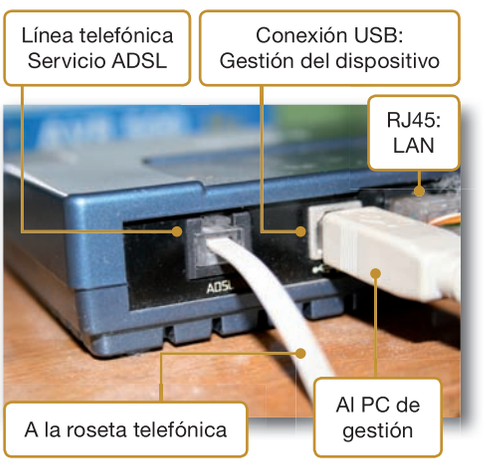


Fig. 5.1. *Detalle de la vista posterior de un router/módem ADSL en producción.*

B. Módems de cable

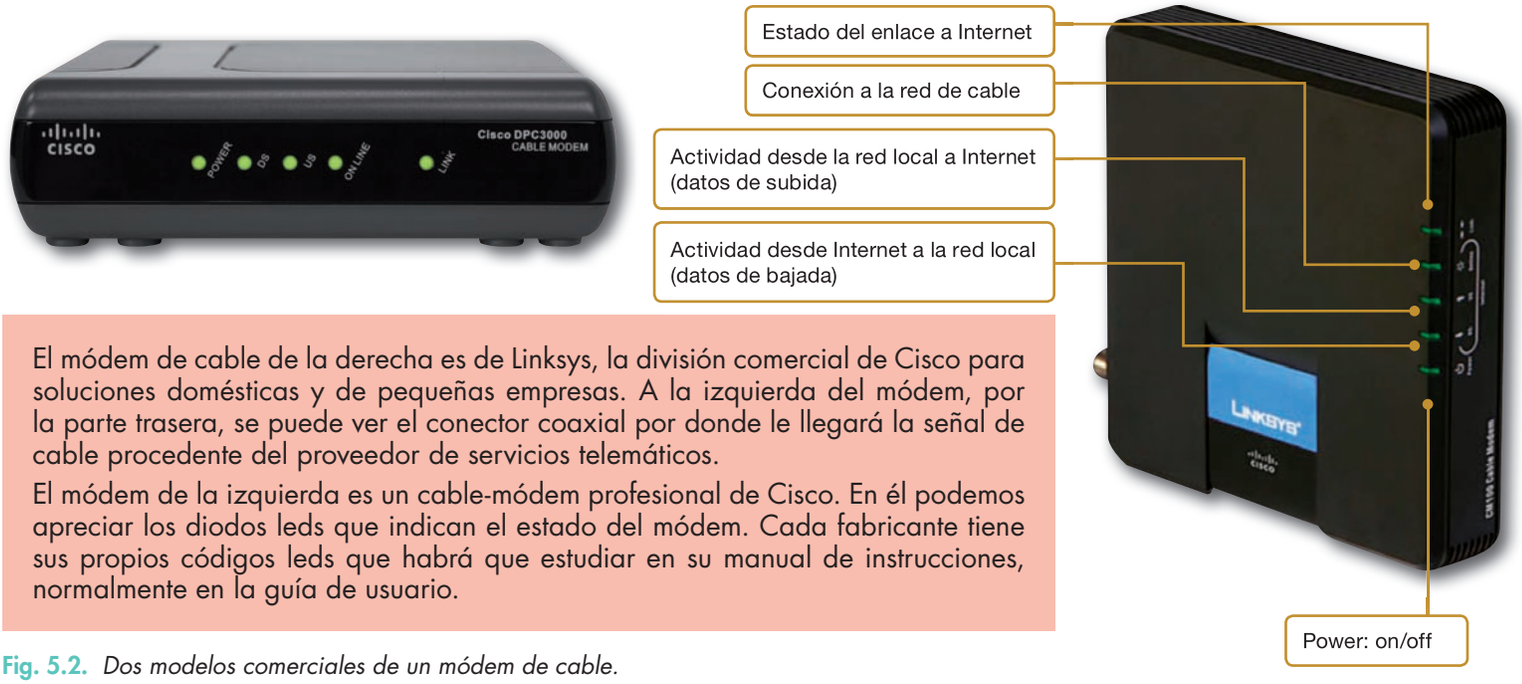
Un módem de cable o cable-módem es un dispositivo que nos permite acceder a Internet a alta velocidad utilizando la infraestructura de las redes de televisión por cable.

Las velocidades de transmisión son muy variables, pero suelen estar entre los 300 Kbps y los 10 Mbps, aunque la tecnología permitiría transmisiones hasta los 40 Mbps.

Los usuarios pueden estar recibiendo sus canales de televisión y simultáneamente estar transmitiendo o recibiendo datos de Internet.

Actividades

1. Busca los errores técnicos en el siguiente razonamiento: «Mi portátil tiene integrado un módem analógico. He contratado un acceso ADSL con mi compañía telefónica y me han comunicado que me lo servirán por mi línea de teléfono analógica. Para evitar tener que comprar un módem ADSL, utilizaré mi módem que, al ser analógico, es compatible con el servicio ADSL que me envían por mi línea de teléfono analógica.»



El módem de cable de la derecha es de Linksys, la división comercial de Cisco para soluciones domésticas y de pequeñas empresas. A la izquierda del módem, por la parte trasera, se puede ver el conector coaxial por donde le llegará la señal de cable procedente del proveedor de servicios telemáticos.

El módem de la izquierda es un cable-módem profesional de Cisco. En él podemos apreciar los diodos leds que indican el estado del módem. Cada fabricante tiene sus propios códigos leds que habrá que estudiar en su manual de instrucciones, normalmente en la guía de usuario.

Fig. 5.2. *Dos modelos comerciales de un módem de cable.*

Ejemplos

Análisis de la configuración de un encaminador ADSL

La configuración de un dispositivo ADSL es muy frecuente en la práctica profesional puesto que cualquier empresa o particular que requiera una conexión a Internet tendrá uno de estos dispositivos.

A veces, el operador del servicio nos lo configurará de modo semiautomático, pero si fuera necesario tener un control exhaustivo de los parámetros de configuración de red, tendríamos que configurarlo nosotros mismos personalmente.

En el caso del router ADSL, se conecta directamente a la red pues estos encaminadores tienen, además de la interfaz telefónica para ADSL, otra interfaz Ethernet para su conexión a la red corporativa. El router que hemos elegido en este ejemplo es gestionable a través del explorador de Internet puesto que incorpora un servidor web a través del cual se puede configurar.

En la Fig. 5.3 podemos ver dos fichas: el resumen de configuración y el resumen de los servicios que proporciona. Podemos observar los parámetros IP de las dos interfaces del módem (el de ADSL y el de Ethernet), así como parte de la configuración de ATM, la banda ancha en la que termina por desembocar ADSL (parámetro VPI/VCI). Además, podemos ver que el router proporciona a la red corporativa los servicios de DNS y el de NAPT, en el que se profundizará más adelante.

Truco

Frecuentemente, los operadores de ADSL proporcionan a sus clientes módems ADSL en vez de routers ADSL. La diferencia más significativa entre ellos reside en el modo en que se conecta a nuestra instalación de red. En el caso del módem ADSL se suele conectar por su puerto USB a un ordenador de la red que hace las funciones de servidor de comunicaciones, comportándose de modo semejante al módem analógico, pero conservando todas las características de la banda ancha.

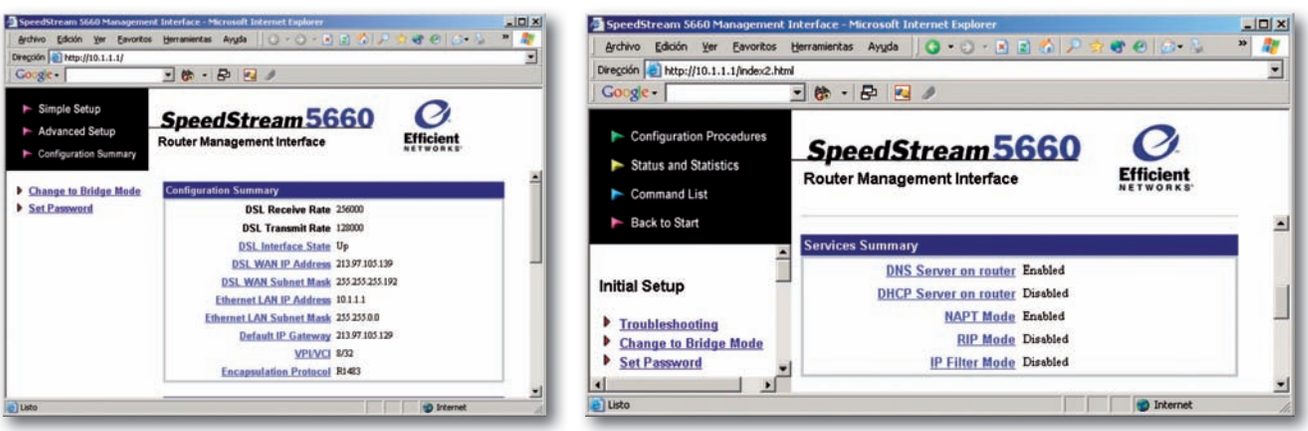


Fig. 5.3. *Fichas de resumen de configuración y servicios en un router ADSL.*

Continúa…

Ejemplos

…Continuación

En la Fig. 5.4 se especifican algunos detalles más sobre las configuraciones de las dos interfaces de red. La mayor parte de estos parámetros son proporcionados por el proveedor del servicio ADSL.

Nosotros solo tendremos que configurar la dirección IP del router en su interfaz de conexión a nuestra red corporativa, que en nuestro ejemplo es 10.1.1.1 con máscara 255.255.0.0.

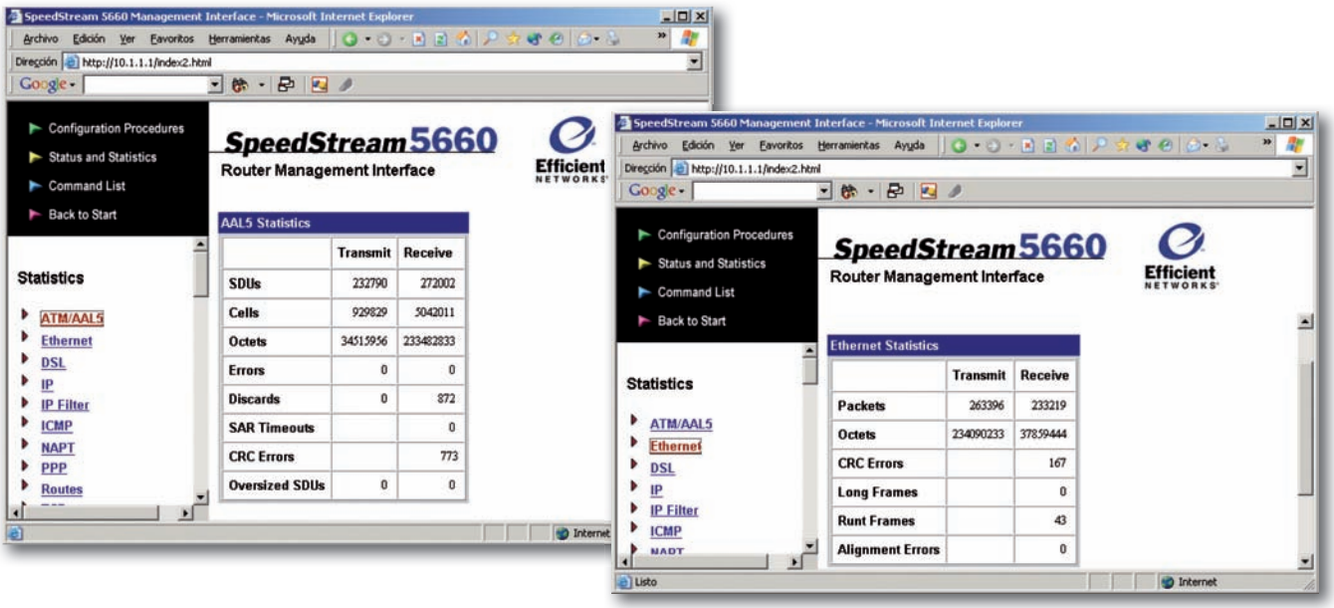


Fig. 5.4. *Detalles de configuración de las interfaces de red de un router ADSL.*

Una vez que el router está funcionando, el administrador podrá consultar las estadísticas de conexiones y estudiar su rendimiento. En la Fig. 5.5 tenemos dos detalles de estas estadísticas, la primera de ellas (a la izquierda) para la red ATM (que es la red de transporte utilizada por la tecnología ADSL) y la segunda (a la derecha) para la interfaz Ethernet que es la utilizada en la conexión a la red corporativa local: el encaminador se encarga de traspasar paquetes entre estas dos redes según unas reglas determinadas por el administrador del router y el servicio prestado por el proveedor telemático.

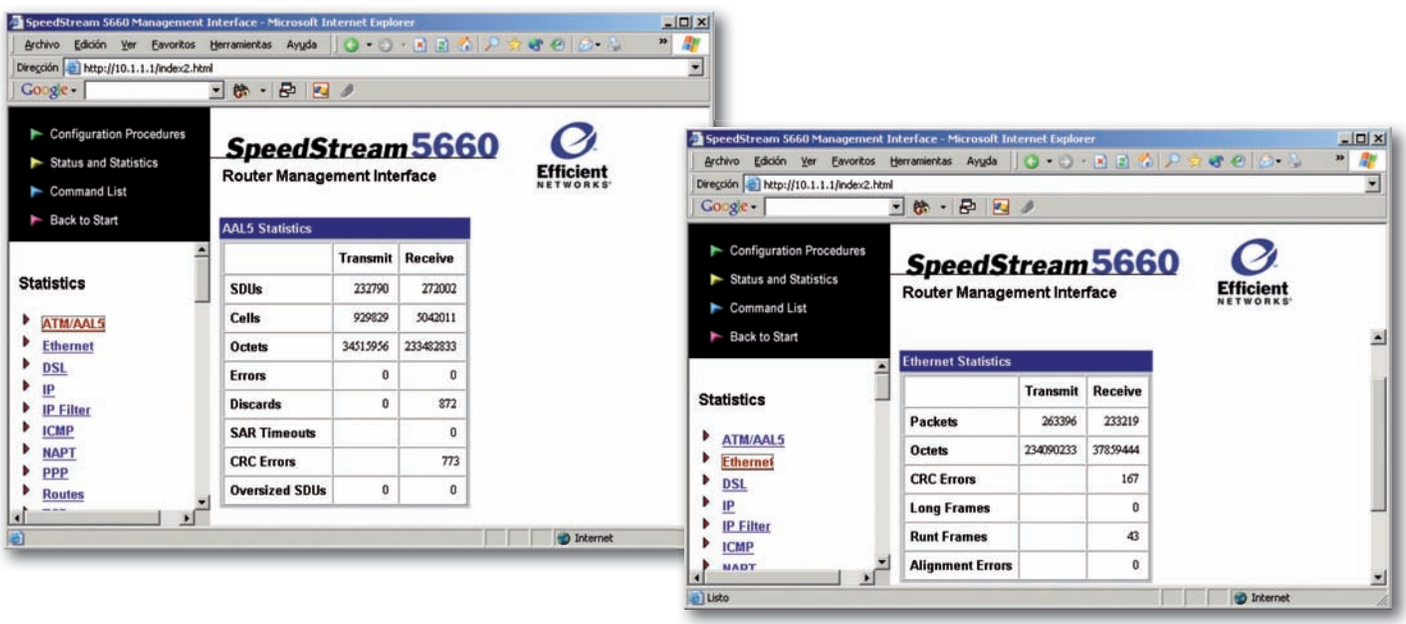


Fig. 5.5. *Fichas de estadísticas de transmisión en un router ADSL.*

Caso práctico 1

Configurando un acceso a Internet por módem

Como ejemplo, vamos a crear un acceso a Internet en el PC utilizando el asistente del acceso telefónico a redes. Aunque en la actualidad la inmensa mayoría de los accesos a Internet son de banda ancha (normalmente ADSL), es interesante conocer cómo se configura una conexión a Internet utilizando un módem analógico.

Es una situación que puntualmente puede resolver el problema de una caída en los dispositivos ADSL de las centrales telefónicas, sustituyendo estas conexiones habituales por un acceso vía módem para comunicaciones críticas o de urgencia mientras el proveedor de Internet soluciona sus problemas.

También puede resolver problemas de conexión en lugares en donde no hay cobertura de banda ancha pero en los que sí llega una línea telefónica analógica. La idea principal es poder tener un acceso a Internet, aunque sea de muy baja calidad, en cualquier sitio en donde haya una roseta de teléfono.

1. En primer lugar, crea una conexión nueva en el panel de control de *Conexiones de red* (Fig. 5.6, arriba a la izquierda). Windows separa las conexiones de acceso telefónico (arriba) de las conexiones de redes de área local (abajo).
2. Una vez que ejecutas el asistente, aparecerán las fichas que se describen en la Fig. 5.7, en las que vas a informar a Windows de que quieres realizar una conexión a Internet (a la izquierda) y, haciendo clic en *Siguiente,* que vas a establecer la conexión manualmente; de este modo te permitirá agregar la información suministrada por el proveedor de la cuenta de acceso.
3. A continuación, elige la asignación de un módem como medio para realizar la conexión y proporciona un nombre a la misma (Fig. 5.8) haciendo clic en *Siguiente*. Con este nombre, Windows fabricará un icono que será el que tengas que activar para realizar posteriormente la conexión.

Ya está configurada la parte de la conexión que tiene que ver con el módem, pero aún falta la asignación de los valores que el proveedor nos proporcionó cuando solicitamos la cuenta de acceso.

Fig. 5.6. *Ventana de conexiones de red de Windows XP y 7.*

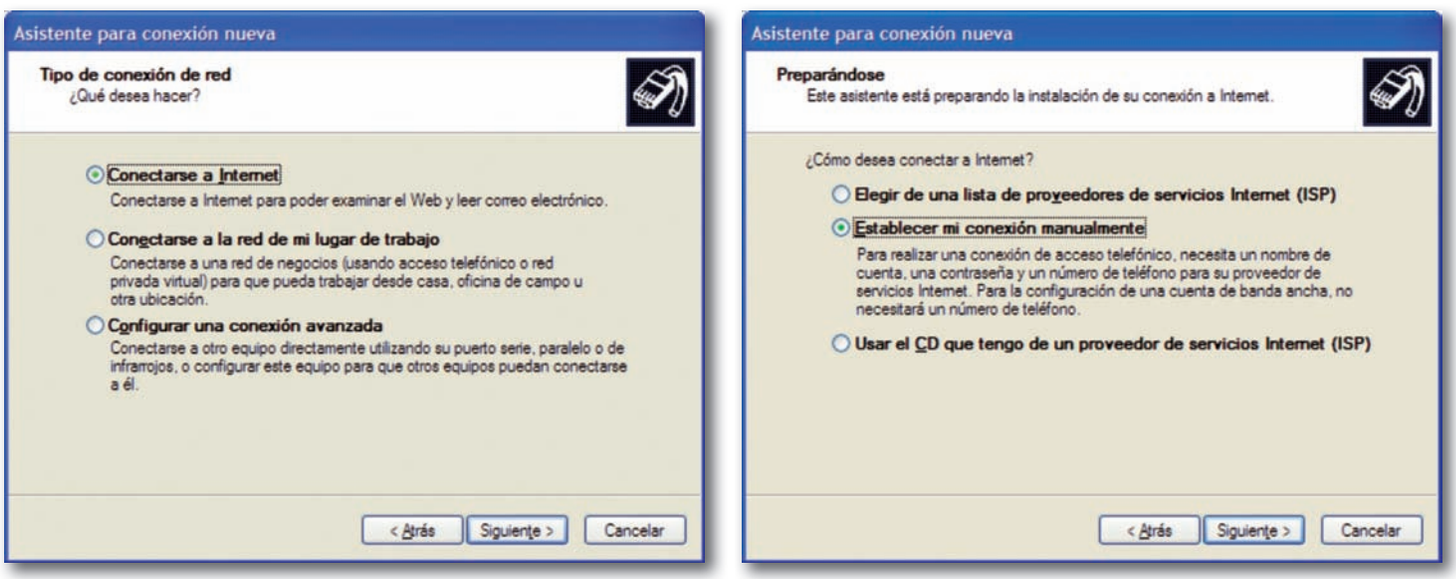


Fig. 5.7. *Asistente de creación de una conexión nueva en Windows.*

Continúa...

Caso práctico 1

...Continuación

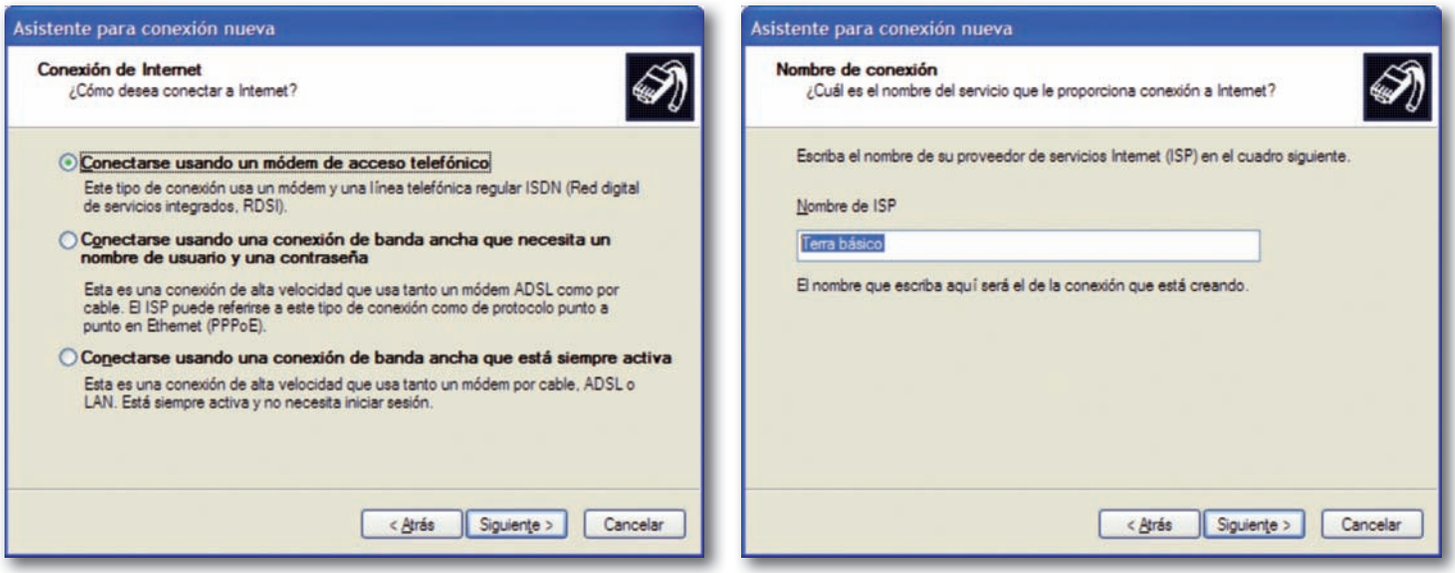


Fig. 5.8. *Asignación del módem y denominación de la conexión.*

4. En la Fig. 5.9 asigna el número de teléfono al que tenemos que marcar, el nombre de usuario y la contraseña de acceso. Estos tres datos te los tiene que proporcionar el proveedor de Internet.

   Además, podemos hacer que este usuario y contraseña sean utilizados por cualquier usuario del equipo, que esa sea la conexión que se marque por defecto o indicarle al cortafuegos del equipo que se haga cargo de vigilar la conexión.

Truco

Si vamos a llamar a través de una centralita, tendremos que incorporar los prefijos adecuados para que la centralita pueda conmutar la llamada que hacemos (interna) con una línea externa. Es muy típico de las centralitas tener que marcar un «0», esperar un tono continuo de conexión con el exterior y solo después marcaremos el número de destino.

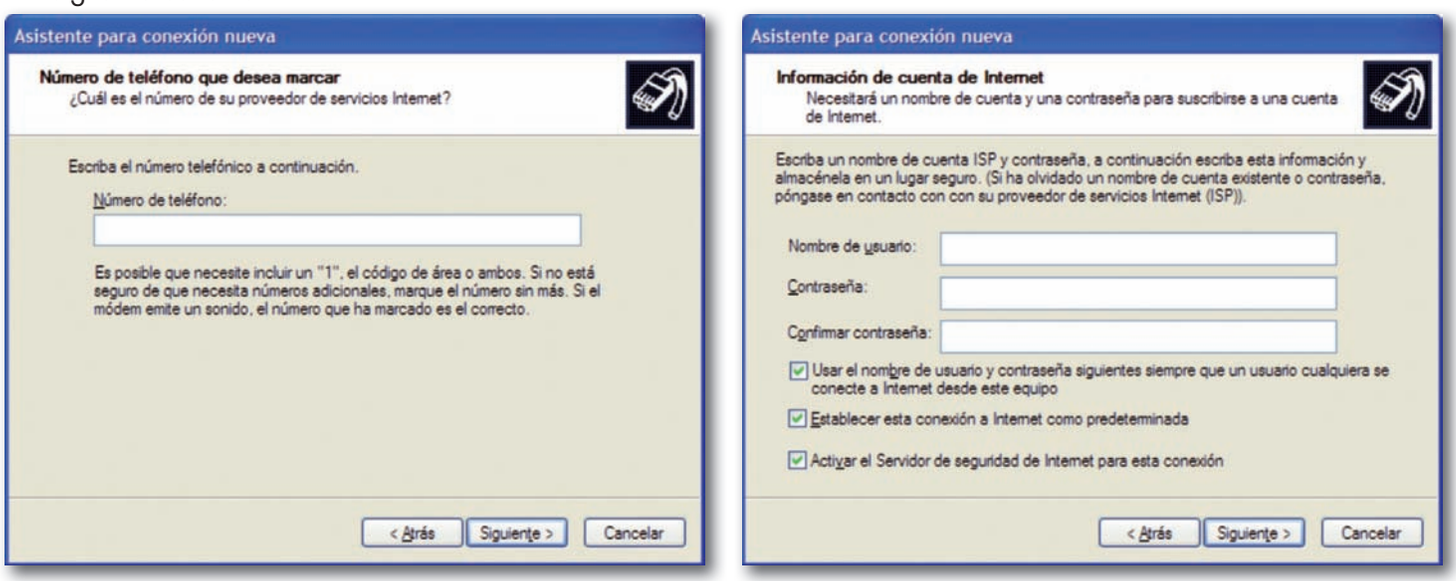


Fig. 5.9. *Asignación del número de teléfono y de la identificación del usuario de la conexión.*

5. Llegados a este punto, el asistente crea la conexión con los parámetros que le hemos proporcionado. Ahora solo falta la incorporación de los parámetros de la red TCP/IP a la que te vas a conectar. Estos parámetros los puedes editar desde las propiedades de la nueva conexión recién creada (Fig. 5.10).

Continúa...

Caso práctico 1

...Continuación

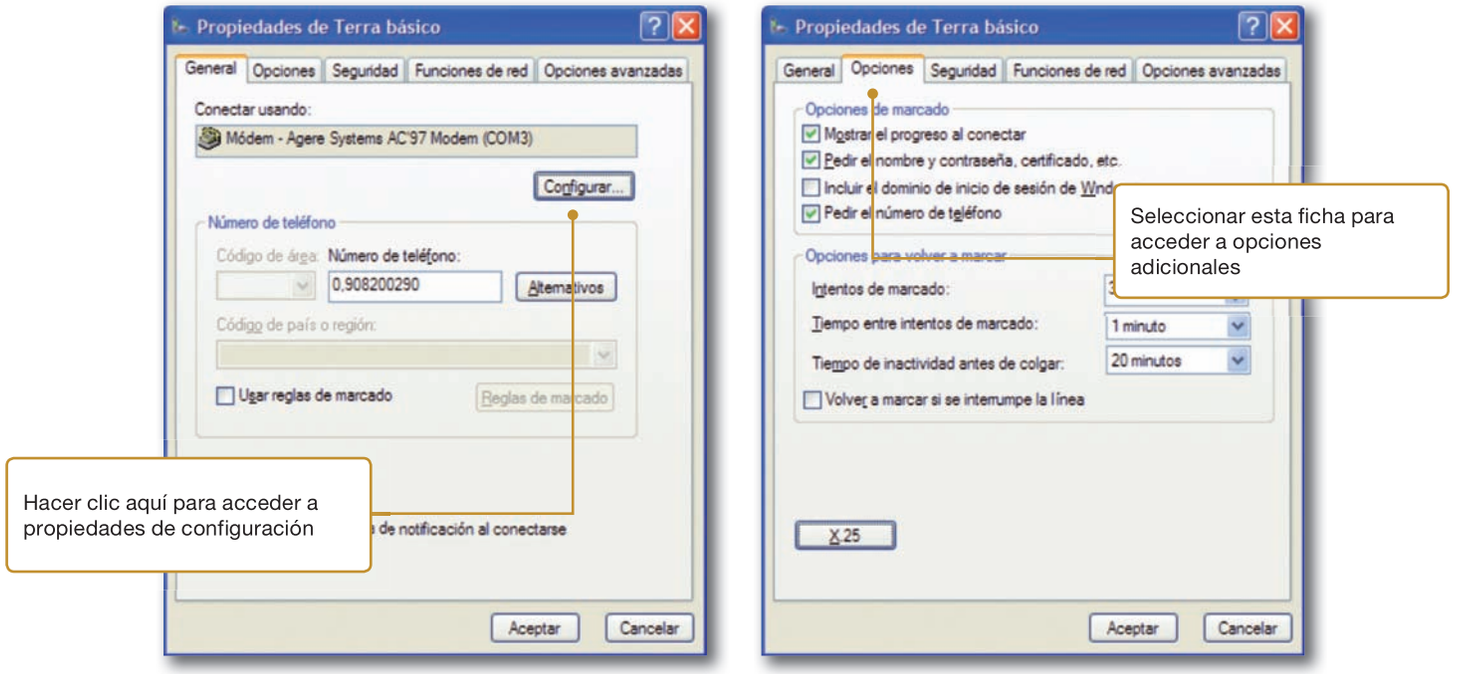


Fig. 5.10. *Propiedades de la conexión telefónica: fichas General y Opciones.*

6. Después puedes especificar si el proveedor requiere o no una contraseña segura (o cifrada) o bien si se podrá utilizar una tarjeta inteligente para la identificación de la conexión. Además, en la ficha de funciones de red puedes ajustar los parámetros del protocolo TCP/IP (Fig. 5.11).

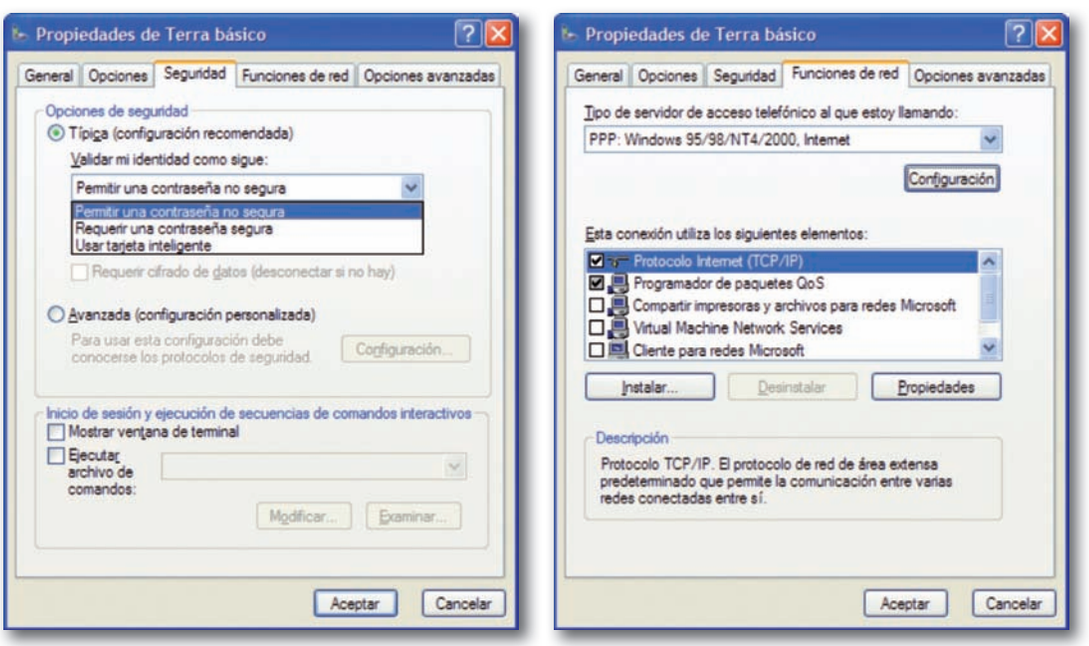


Fig. 5.11. *Fichas de identificación del usuario y definición de los elementos de red utilizados en la conexión.*

Continúa...

Caso práctico 1

...Continuación

7. Si seleccionas el protocolo TCP/IP y haces clic en el botón de propiedades, aparecerá algo semejante a la ventana que vemos en la Fig. 5.12. En esta ficha le has dicho a Windows que el proveedor nos asignará la dirección IP automáticamente. Si no fuera así, el proveedor te diría qué valor tienes que escribir aquí.

   También has asignado las direcciones de los dos servidores DNS que nos especificó el proveedor. A veces el proveedor también asigna los DNS automáticamente.

Claves y consejos

Cuando se contrata un servicio de comunicaciones con un operador, este debe especificarnos los parámetros de conexión adecuados que debemos utilizar. En muchos casos, el operador nos asignará estos parámetros automáticamente al identificarnos en el servicio.

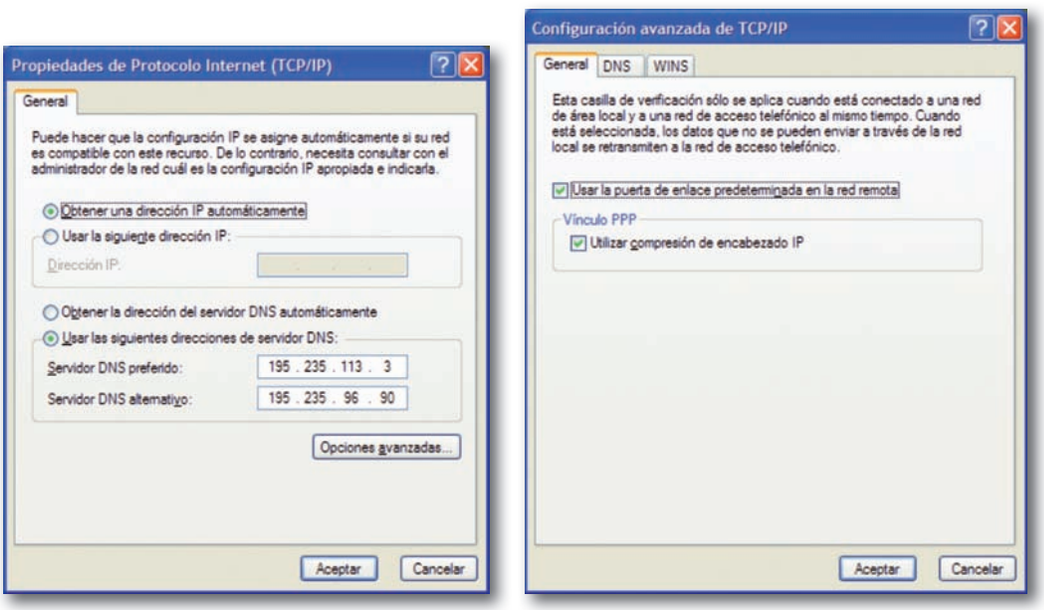


Fig. 5.12. *Fichas de configuración del protocolo TCP/IP en una conexión de red por acceso telefónico.*

8. En las opciones avanzadas puedes terminar de ajustar el TCP/IP. Habitualmente, salvo que el proveedor diga lo contrario, serán suficientes los valores por defecto que Windows sugiere. Con estas operaciones acaba el procedimiento de configuración del acceso de red.
9. Ahora solo te falta probar la conexión haciendo doble clic en el icono que Windows habrá creado en las *Conexiones de red;* aparecerá en pantalla la ficha de identificación de usuario y el número de teléfono que se debe marcar (Fig. 5.13).

   Podemos validar la información de conexión que Windows nos presenta o modificarla como sea necesario. La conexión se iniciará cuando hagamos clic sobre el botón *Marcar.*

Esto mismo puede hacerse fácilmente en un sistema Linux, aunque el modo concreto de hacerlo dependerá de la distribución de Linux de que se disponga y de la versión. Si el módem analógico es externo, no suele haber dificultades especiales ya que el módem funcionará con solo encenderlo y únicamente tendremos que ocuparnos de configurar las comunicaciones con él por el puerto serie del PC que ejecute Linux.

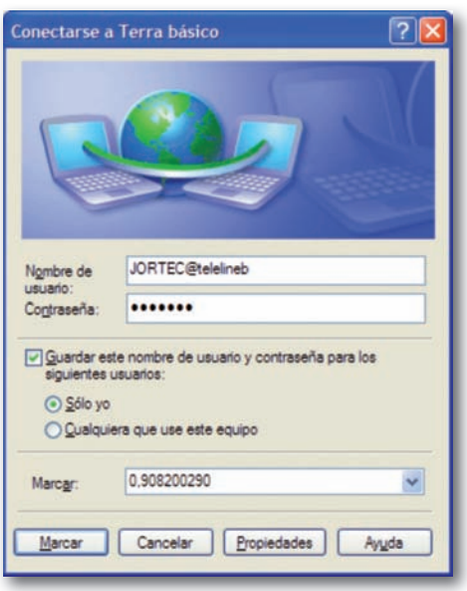


Fig. 5.13. *Ventana de conexión por acceso telefónico en un sistema Windows.*

Continúa...

Caso práctico 1

...Continuación

En cambio, si el módem es interno la dificultad mayor reside en encontrar los controladores apropiados para el módem, que deberán estar escritos específicamente para el hardware del módem.

Frecuentemente estos controladores se encuentran con mayor dificultad en Linux que en Windows, sobre todo si se trata de módems más modernos.

Una vez que el sistema operativo Linux haya reconocido el módem podremos configurar la conexión en la ficha de *Configuración de la red* (Fig. 5.14-A), a la que se puede acceder desde el submenú de administración del menú de sistema. En ella seleccionaremos la conexión por módem que aparezca.

Hay que fijarse en que la interfaz de comunicaciones que utilizará Linux es ppp0 *(point to point protocol),* para protocolos de conexión punto a punto.

En las propiedades de la conexión de módem, podremos activar o desactivar la conexión, configurar el número de teléfono, el prefijo de marcado y los datos de identificación de usuario: nombre y contraseña asignados por el proveedor del servicio de conexión (Fig. 5.14-B).

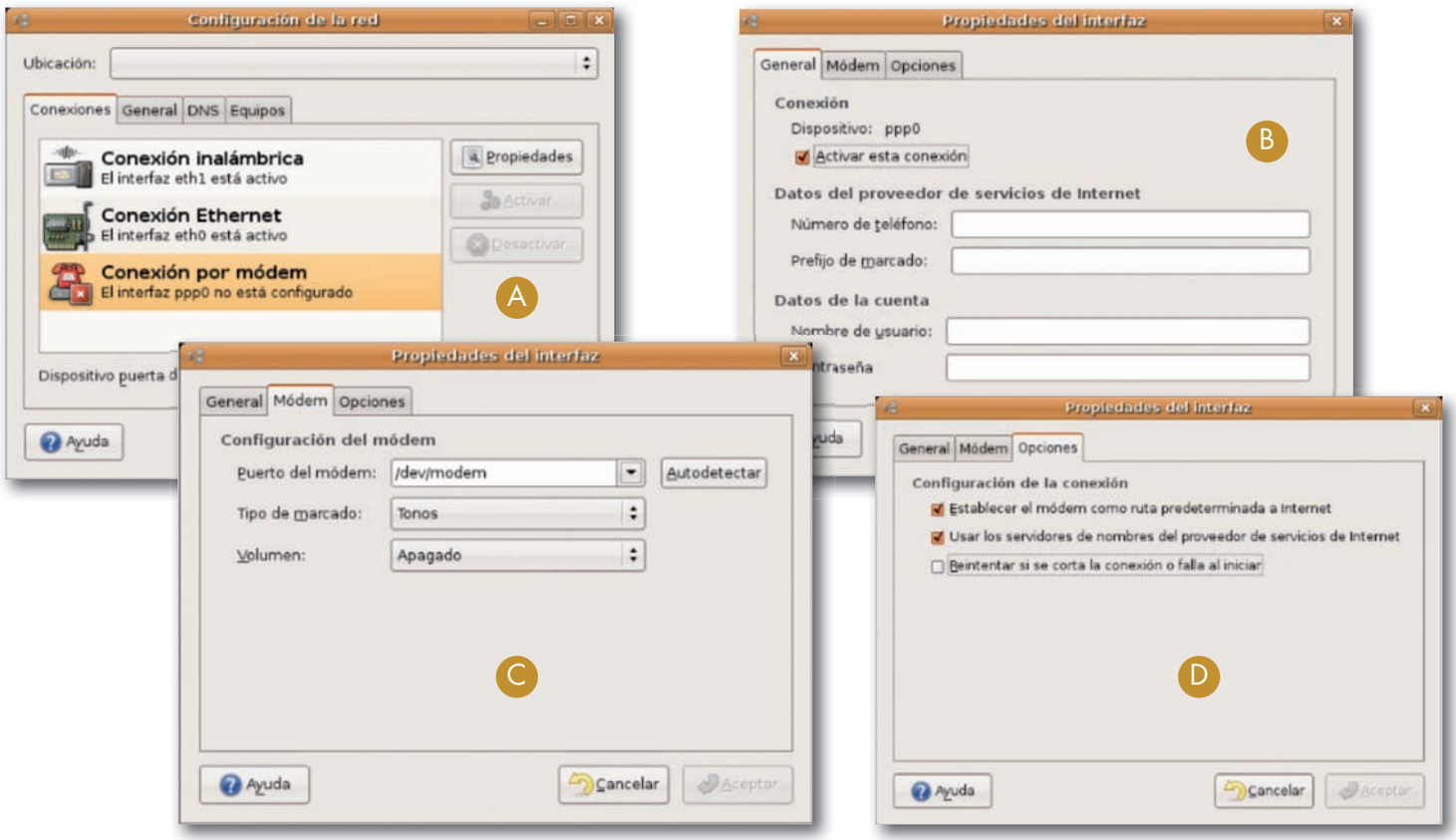


Fig. 5.14. *Configuración de un módem en Ubuntu (A). Ficha de configuración general de la conexión (B). Fichas de gestión de módem (C) y opciones de red (D) en la configuración de una conexión por módem en Ubuntu.*

En la ficha de la Fig. 5.14-C podremos configurar algunos parámetros de modo automático si Linux es capaz de autodetectar nuestro módem, así como asignar si queremos que este marque por tonos o por pulsos y ajustar el volumen del altavoz. En esta ficha también aparece el nombre del puerto utilizado por el módem para su comunicación con el sistema operativo: en nuestro caso */dev/modem* que se corresponde con un módem interno.

Por último, en la ficha de configuración de *Opciones,* podremos indicarle al sistema operativo que para enviar paquetes al exterior del PC utilice los parámetros de red de la conexión por módem en vez de las propias de la red de área local procedentes de otras posibles interfaces de red (Fig. 5.14-D).

En el caso de esta figura se utilizará la ruta predeterminada a Internet (puerto por defecto de la conexión) y los servidores de nombres que proporcione el proveedor (servidores DNS o de nombres NetBIOS).

Vocabulario

Instalación en cascada: se dice que un conjunto de dispositivos están instalados en cascada o de modo jerárquico cuando unos están conectados a los otros de modo que la salida de uno es la entrada de otro.

2. Repetidores y concentradores

Las señales eléctricas se degradan al transmitirse. Cuando la longitud del cable de red es grande, la señal puede llegar al otro extremo casi imperceptible, lo que origina problemas graves en las transmisiones. El modo más básico de solucionar estos problemas consiste en la utilización de **repetidores** o concentradores ***(hubs).***

El repetidor es un elemento de red que regenera la señal eléctrica que le llega con el fin de restituir su nivel original, y así evitar los problemas que se pudieran producir por una excesiva atenuación.

Teóricamente es posible instalar tantos repetidores en una red como sean necesarios, sin embargo, hay serias razones que impiden su **instalación en cascada** en gran número.

Los repetidores operan en el nivel físico, puesto que trabajan con señales. Esto hace que sean rápidos, aunque no puedan procesar los datos que circulan a través de ellos.

En ocasiones, los repetidores se pueden utilizar para convertir la señal de un sistema de cableado en otro. Por ejemplo, un repetidor podría tener una entrada 10Base2 (coaxial) y otra 10BaseT (par trenzado).

Los repetidores operan en el nivel físico, puesto que trabajan con señales. Esto hace que sean rápidos, aunque no puedan procesar los datos que circulan a través de ellos.

En ocasiones, los repetidores se pueden utilizar para convertir la señal de un sistema de cableado en otro. Por ejemplo, un repetidor podría tener una entrada 10Base2 (coaxial) y otra 10BaseT (par trenzado).

Fig. 5.16. *Distintos modelos de repetidores.* Hub *doméstico (abajo, a la izquierda). Transceptor 10Base2/10Base5 (abajo, a la derecha). Obsérvese cómo el repetidor tiene en la parte superior una interfaz coaxial y en el frontal varios puertos RJ45 para intercambiar señales entre estos dos distintos tipos de red. El transceptor adecúa la señal de su canal coaxial al de pines.*

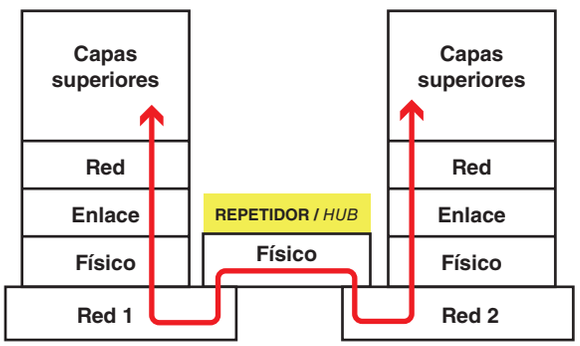


Fig. 5.15. *Modelo de capas para un repetidor o* hub. *El repetidor opera con señales por eso es un dispositivo que solo contempla la capa física para unir los nodos origen y destino.*

La ventaja principal de un *hub* reside en la facilidad de operación: se limita a copiar bits de un segmento de red en otros. No requiere ningún tipo de configuración especial puesto que opera en el nivel físico. No atiende a las direcciones de red, protocolos, servicios, etc. Sencillamente repite la señal de la red a gran velocidad.

La mayor limitación del *hub* consiste en que no aísla de los problemas del tráfico generados en la red en cada uno de los segmentos: si en uno de los segmentos se produce una colisión, esta se propagará por todos los segmentos de la red.

Actividades

2. Una red local está compuesta por varios segmentos de red. Los segmentos están unidos por medio de un dispositivo de interconexión. Una estación de la red está infectada por un virus de tipo gusano y está generando mucho tráfico Ethernet en el segmento de red en que está la estación. ¿Pasa ese tráfico de un segmento a otro si el dispositivo de interconexión es un concentrador? ¿Y si fuera un repetidor?

3. Seguimos trabajando sobre la configuración de red del ejercicio precedente. Ahora vamos a suponer que el cableado de red es coaxial y lo que ocurre es que se rompe uno de los segmentos de red. Como la red queda abierta, el segmento de red en que se ha producido la rotura deja de funcionar. ¿Funcionarán el resto de los segmentos de red si el dispositivo de interconexión es un repetidor? ¿Y si la red fuera de cable de pares en vez de coaxial y el dispositivo de interconexión fuera un concentrador?

3. Puentes

El **puente** o *bridge* es un elemento de cierta capacidad de control. Puede aceptar y reexpedir las tramas que le llegan en función del contenido de las mismas. La instalación de un puente en una red de área local es justificable, por ejemplo, cuando se desea aislar el tráfico en cada segmento de red que conecta el puente.

Los puentes operan en nivel 2 de OSI, es decir, su unidad de operación básica es la trama de red (Fig. 5.17). Cuando un puente debe pasar una trama de un segmento a otro de la red ejecuta las siguientes fases:

- Almacena en memoria la trama recibida por cualquier puerto para su análisis posterior.
- Comprueba el campo de control de errores de la trama con el fin de asegurarse de la integridad de la misma. Si encontrara un error, eliminaría la trama de la red, con lo que tramas incompletas o erróneas no traspasarán la frontera del segmento de red en donde se produjo el fallo.
- Algunos puentes son capaces de retocar de modo sencillo el formato de la trama (añadir o eliminar campos) con el fin de adecuarla al formato del segmento destinatario de la misma.
- El puente reexpide la trama si determina que el destinatario de esta se encuentra en un segmento de red accesible por alguno de sus puertos.

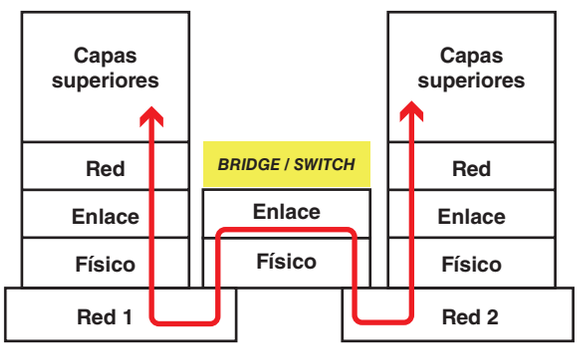


Fig. 5.17. *Modelo de capas para un puente o un conmutador. El* switch *opera con tramas por eso es un dispositivo que trabaja en la capa de enlace para unir los nodos origen y destino.*

Puesto que los puentes operan en el nivel 2, no pueden tomar decisiones de encaminamiento que afecten a los protocolos o sistemas de direccionamiento del nivel 3: solo pueden operar con direcciones de nivel 2 (direcciones MAC). A este aislamiento de tráfico que se opera en los puentes o en dispositivos de red de nivel superior se le suele denominar «separación de los **dominios de colisión**» ya que dos estaciones situadas en diferentes segmentos no pueden colisionar en su acceso a la red, puesto que las tramas no pueden atravesar la frontera de los segmentos de red salvo que un puente tome la decisión de conmutarlas.

Actividades

4. Descubre los errores técnicos en el siguiente argumento: «en mi oficina hay dos departamentos claramente diferenciados. En cada uno de ellos se genera mucho tráfico, pero apenas tienen relación entre sí. Se ha pensado en instalar un puente entre las dos redes departamentales, pero no hemos podido puesto que las dos redes están en el mismo edificio y los puentes solo pueden operar remotamente».

5. Una compañía tiene sede en dos ciudades, pero solo poseen una red local compartida entre las dos sedes y conectadas por un puente de red a través de redes públicas. El segmento de red de una de las ciudades es minoritario, pero en la otra sede residen los servidores y en su segmento de red se produce mucho tráfico local. ¿Pasará ese tráfico al segmento de red minoritario? Un usuario de la sede minoritaria quiere enviar un fichero al servidor que reside en la sede mayoritaria a través del puente. A pesar de que el puente aísla del tráfico local, ¿podrá hacerlo?

Vocabulario

Dominio de colisión: dos nodos de red pertenecen al mismo dominio de colisión si sus tramas pueden interferir entre sí.

Ampliación

El repetidor, a diferencia del puente, no puede aislar del tráfico broadcast que se genere en la red, ya que difunde cualquier trama que llegue a cualquiera de sus puertos. Esto puede llevar a congestiones serias de la red. Por tanto, un repetidor nunca divide un dominio de colisión y no será capaz de parar las tormentas de tramas de multidifusión.

Tradicionalmente se han clasificado los puentes en transparentes y no transparentes:

- Un puente transparente o de árbol de expansión es un puente que no requiere ninguna configuración para su funcionamiento. Determina la reexpedición de tramas en función de los sucesos que observa por cada uno de sus puertos.
- Un puente no transparente necesita que la trama lleve información sobre el modo en que debe ser reexpedido.

Una segunda clasificación para los puentes se fija en si las dos redes a conectar están o no próximas. Según esto los puentes pueden ser:

- Locales. Un puente local aglutina en sí mismo dos o más segmentos de la misma red.
- Remotos. Un puente remoto está dividido en dos partes. Cada una de estas partes conecta un segmento de red y las dos partes están interconectadas a través de la línea de una red WAN, por ejemplo, una línea de teléfono o RDSI.

Investigación

Los conmutadores son en la actualidad los dispositivos más utilizados para realizar el despliegue de la red: repetidores y concentradores solo se utilizan en casos muy específicos y siempre minoritarios. Los *switches* incorporan muchas otras funciones además de la conmutación de tramas que es en la que se especializan.

Puedes investigar algunos ejemplos de estas tecnologías en Wikipedia por la voz «switch» y, más en concreto, en la tecnología «spanning tree».

Ampliación

Aunque el aspecto externo de un *hub* coincide con el de un *switch* y, efectivamente, ambos distribuyen señal entre segmentos de red, hay diferencias sustanciales entre ellos. La más significativa es que mientras que en el *hub* el ancho de banda es compartido por todos los puertos mediante una multiplexación en el tiempo (solo una estación puede transmitir de un puerto a otro en cada instante), en el *switch* el ancho de banda está por encima del ancho de banda de cada uno de los puertos. De hecho, en los conmutadores de muy alto rendimiento, el ancho de banda del *backplane* (el bus interno que intercomunica todos los puertos del conmutador) es al menos la suma de los anchos de banda de cada uno de los puertos, con lo que se garantiza que la conmutación será de alta velocidad, y que unos segmentos de red no interferirán en los otros. En un *switch* cada puerto representa un dominio de colisión diferente.

4. Conmutadores

El *switch* o conmutador es un dispositivo que tiene funciones del nivel 2 de OSI y que, por tanto, se parece a un *bridge* en cuanto a su funcionamiento. Sin embargo, tiene algunas características que lo distinguen:

- El *switch* es siempre local.
- Son dispositivos multipuerto.
- La velocidad de operación del *switch* es mayor que la del puente remoto, que introduce mayores tiempos de retardo al tener que utilizar una conexión WAN entre los dos segmentos de la LAN que interconecta.
- En un conmutador se puede repartir el ancho de banda de la red de una manera apropiada en cada segmento de red o en cada nodo, de modo transparente a los usuarios. Esto proporciona facilidades para la construcción de redes virtuales, que trataremos más adelante.
- Gran parte de los modelos comerciales de conmutadores son apilables y, por tanto, fácilmente escalables, lo que les da una flexibilidad semejante a los repetidores, pero con la funcionalidad de los puentes en cuanto a la gestión del tráfico de red se refiere.
- Algunos conmutadores de muy alto rendimiento se conectan en forma modular a un bus de muy alta velocidad *(backplane)* por el que producen su conmutación.

Las tecnologías de conmutación han avanzado de tal modo que en la actualidad se comercializan también conmutadores de nivel 3 o superior. Un conmutador de nivel 3 incorpora funciones de encaminamiento pero con la velocidad de la conmutación.

En la Fig. 5.18 puede verse el modo de funcionamiento de un *switch*. El conmutador construye una tabla por cada puerto con las direcciones físicas de los dispositivos que ve por cada uno de ellos. Cuando le llega una trama, investiga en estas tablas para averiguar por qué puerto de todos los disponibles alcanza su destino transmitiéndola por ese puerto y solo por ese, a diferencia del *hub* que la transmitiría por todos los puertos disponibles salvo por el puerto por donde llegó.

Por ejemplo, si al *switch* le llega una trama cuya dirección física de destino es MAC4, el conmutador buscará esa dirección entre sus tablas de direcciones, la hallará disponible en el puerto 2 y conmutará la trama para que salga por ese puerto. La trama llegará al *hub* que está conectado a ese puerto segundo y el *hub* la transmitirá por todos sus puertos llegando a las estaciones PC4 (su destino) y PC5.

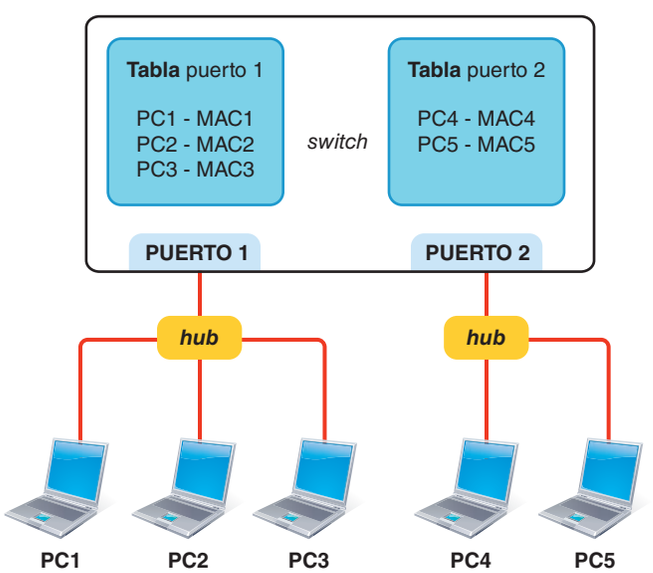


Fig. 5.18. *Tablas de direcciones físicas en los puertos de un conmutador.*

Los conmutadores son gestionables por los protocolos típicos de gestión de red: **SNMP, RMON,** etc. Evidentemente, si se hace depender gran parte de la eficacia de la red de unos conmutadores, interesará que la vigilancia de estos sea muy estrecha. La mayoría de los *switches* pueden también gestionarse vía web porque incorporan un servidor web desde donde realizar su configuración, así como a través de conexiones telnet o ssh.

En la Fig. 5.19 podemos ver cómo el *switch* tiene sus parámetros de red TCP/IP como cualquier otro nodo de la red: dirección IP, máscara, puerta por defecto, etc.

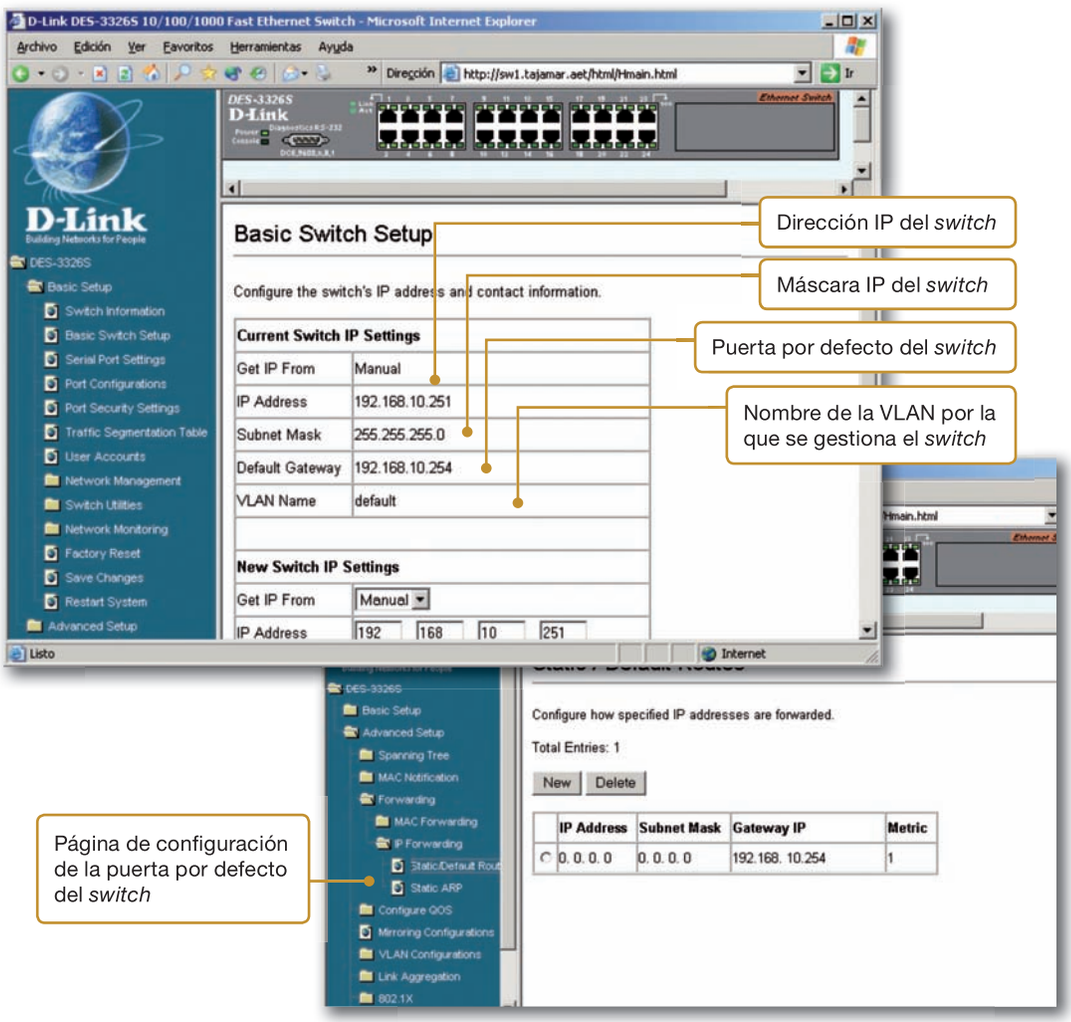


Fig. 5.19. *Fichas de configuración web de los parámetros básicos de un conmutador gestionable.*

Finalmente, hay que centrar la atención en el nivel físico de conexión de los puertos del *switch*. La conexión de las estaciones a los puertos de conmutador se hace mediante un cable directo. En cambio, los cables que conectan varios *switches* entre sí requieren cables cruzados. La mayor parte de los *switches* actuales tienen algún puerto especial que hace internamente el cruce de pares de modo que se pueda utilizar también un cable directo para interconectarlo con otro *switch* utilizando este puerto. Estos puertos suelen venir etiquetados con el identificador **MDIX** o **MDI-X** (Interfaz cruzada dependiente del medio, *Medium Dependent Interface Crossover*) para diferenciarlos de los puertos MDI que son los que no hacen *crossover* (puertos normales para conectar mediante cable directo).

En un estadio más avanzado, el puerto puede tener inteligencia suficiente como para admitir tanto una conexión MDI (cable directo) como MDI-X (cable cruzado): en este caso, el identificador del puerto suele ser **MDI/MDI-X.** En cualquier caso, siempre conviene consultar las especificaciones del fabricante para conocer con exactitud las prestaciones de cada puerto.

Truco

Cuando el profesional tiene que elegir la solución comercial concreta de un dispositivo de red, no solo debe fijarse en las prestaciones de rendimiento o el precio, hay muchos otros detalles que complementan la funcionalidad básica del dispositivo que frecuentemente lideran la decisión final.

Actividades

6. Di si son verdaderas o falsas las siguientes afirmaciones:

a) Los conmutadores son más rápidos que los puentes.

b) Un conmutador es siempre local.

c) El conmutador, como el puente, no puede gestionar el ancho de banda.

d) Todos los conmutadores se pueden escalar.

e) La mayor parte de los *switches* se pueden configurar a través de su página web.

7. En la instalación de la red de una oficina se ha propuesto una distribución Ethernet conmutada de los puestos de los usuarios. Inicialmente se han alquilado dos plantas, pero es probable que en un futuro no lejano se tenga que alquilar más espacio para asegurar un crecimiento de la empresa. Esto generará nuevas reconfiguraciones de la red para, sin anular la infraestructura de red inicial, poder ampliar el número de puestos de trabajo con acceso a la red. Teniendo en cuenta que la solución no tiene por qué ser única, ¿qué tipo de *switch* central pondrías en la instalación? Razona la respuesta.

Claves y consejos

En la red de área local se definen varias VLAN entre las que posteriormente se pueden establecer relaciones de más alto nivel, por ejemplo, se podría organizar una VLAN por cada departamento de una corporación de modo que todos los componentes de ese departamento estén lógicamente aislados de otros departamentos. El servidor que utilizan, si es compartido con otros departamentos, deberá pertenecer a varias redes virtuales simultáneamente. También podría habilitarse el encaminamiento entre las distintas VLAN a través de un enrutador en el que se definirán las políticas de comunicación entre los nodos pertenecientes a las distintas VLAN.

5. Tecnologías específicas de los conmutadores

Las redes de área local son muy dependientes del cableado. El cambio de posición geográfica de un usuario de una red supone modificar la configuración del cableado de red, lo que casi siempre es imposible. La tecnología VLAN (léase «vilan») permite que los nodos de la red se conecten a redes lógicas en vez de a redes físicas.

5.1. Redes de área local virtuales o VLAN

Cada VLAN está formada por un grupo lógico de estaciones físicamente unidas a los puertos de uno o más conmutadores que son gestionadas en grupo como si estuvieran en la misma red de área local física.

La pertenencia a una VLAN puede estar asignada manualmente (VLAN estáticas) o hacerse dinámicamente (VLAN dinámicas) mediante un registro automático a través del protocolo GVRP *(Generic VLAN Registration Protocol).* Cada estación solo puede comunicar con otras estaciones de su grupo, aunque no hay inconveniente en que una estación pueda pertenecer a más de un grupo, si el software de gestión lo permite.

Las principales ventajas que proporciona una VLAN son:

- Mejoras en la velocidad de la red por una mejora en la gestión de los puertos de comunicaciones.
- Incremento del ancho de banda o mejora de la asignación del mismo en función de las necesidades.
- Incremento de la seguridad de la red por segregación de usuarios con necesidades especiales o por aislamiento de conexiones que generen excesivo tráfico y que puedan dañar el rendimiento global de la red.
- Generación de grupos de dispositivos con protocolos obsoletos e incompatibles con el tráfico habitual de la red y que se canalizarán a través de una VLAN específica.

Existen varias formas de establecer una VLAN. Cada uno de estos modos proporciona una funcionalidad distinta. Están basados en la tecnología de conmutadores o de encaminadores.

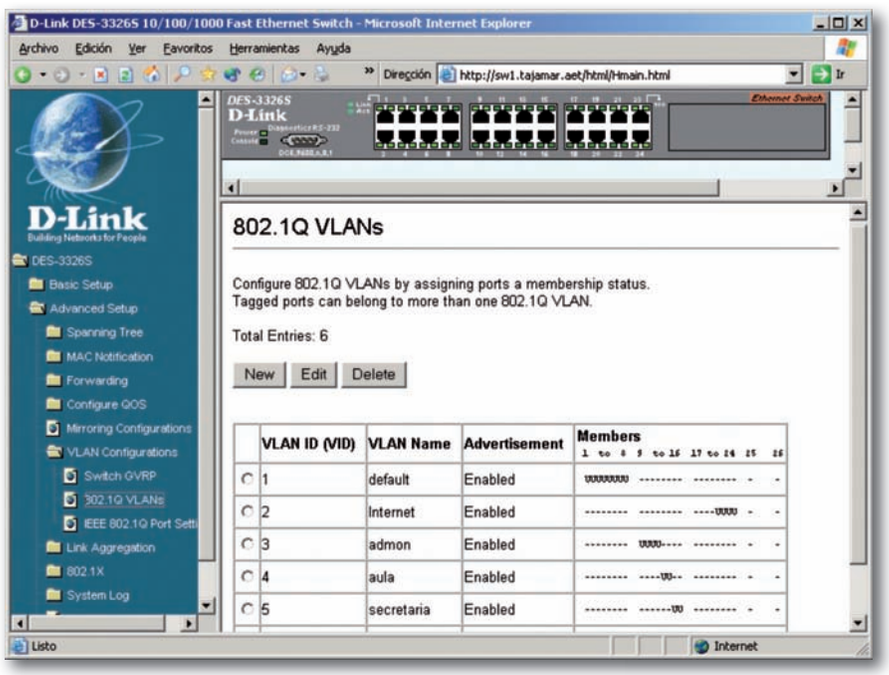


Fig. 5.20. *Creación de VLAN 802.1Q en un conmutador a través de su página web.*

En la Fig. 5.20 podemos observar la página de configuración de VLAN en un conmutador compatible con 802.1Q en el que se han dado de alta seis VLAN distintas por el procedimiento de asignaciones de puertos. Por ejemplo, la VLAN denominada «admon» lleva el identificador número 3 y está compuesta por todos los nodos conectados a los puertos 9, 10, 11 y 12 del conmutador. La letra «U» en la posición del puerto indica que los nodos destinatarios por ese puerto no entenderán tramas 802.1Q y que, por tanto, será el conmutador el encargado de remover la información de *tagging* a la salida de la trama o de insertarla con el identificador 3 a la entrada de la misma.

Las VLAN permiten que los nodos de la red se agrupen según unos criterios lógicos denominados ***policies*** o políticas de conexión que los independizan de su ubicación haciendo que dos nodos que pertenecen a segmentos distintos de la red pertenezcan de hecho a la misma VLAN y puedan comunicar entre ellos transparentemente como si estuvieran en el mismo segmento.

Podemos hacer una sencilla clasificación de tipos de VLAN:

- **VLAN con asignaciones de direcciones MAC.** Los conmutadores de la red crean grupos lógicos con direcciones MAC de los nodos a los que tienen acceso. Cuando una estación cambia de ubicación, sigue manteniendo su dirección MAC y por tanto sigue perteneciendo al mismo grupo virtual, aunque haya cambiado su situación geográfica.
- **VLAN con asignaciones de puertos.** Es una VLAN semejante a la anterior, pero con la peculiaridad de que las asociaciones se realizan agrupando puertos del conmutador en vez de direcciones MAC de los nodos. Todos los nodos del segmento de red conectado por cada puerto asociado a una VLAN pertenecen a esa VLAN.
- **VLAN por direccionamiento virtual.** Las redes virtuales se constituyen sobre nodos que comparten un sistema de direccionamiento, configurándose a través de máscaras de red. Se trata, por tanto, de una extensión de las VLAN al nivel 3 de OSI.

El estándar más frecuente de creación de VLAN es el **IEEE 802.1Q o VLAN *Tagging*.** Gracias a él se pueden definir VLAN a través de la red con independencia del fabricante de los conmutadores. En IEEE 802.1Q cada nodo lleva asociado un número de VLAN a la que pertenecerá con independencia de su ubicación en la red y que se registrará en la cabecera de todas las tramas *(tagging)*, que serán modificadas. Como la configuración de la VLAN reside en la configuración de la tarjeta de red, es necesario que las tarjetas de red sean compatibles con IEEE 802.1Q.

El puerto del conmutador al que se conecta un nodo configurado con IEEE 802.1Q se marca como «Tag».

Otro modo alternativo posible es dejar las tarjetas de red sin configurar y, sin embargo, configurar el puerto del *switch* al que se conecta el nodo para que sea él quien inserte la modificación en la trama que lleva la información de VLAN. En este caso se dice que el puerto del *switch* está configurado como «Untag».

En la Fig. 5.21, a la izquierda, se puede ver la ficha de configuración de prioridades de VLAN para una interfaz de fibra de D-Link en donde asociaremos el identificador de la VLAN (VLAN ID), que es un número, a una prioridad. A la derecha, tenemos la configuración de VLAN de un interfaz de red de Intel en donde se han definido varias VLAN, asociando el número identificador a un texto. Por ejemplo, la VLAN AG1 tiene el identificador 212, la VLAN Infantil el 205, etc. Abajo, se está definiendo la pertenencia a la VLAN número 3 del nodo poseedor de la tarjeta de red que se está configurando. La mayor parte de las VLAN pueden asociar prioridades a las tramas de las diferentes VLAN de modo que se organice un sistema de calidad de servicio. El protocolo comúnmente utilizado para llevar a cabo esto es **IEEE 802.1P.**

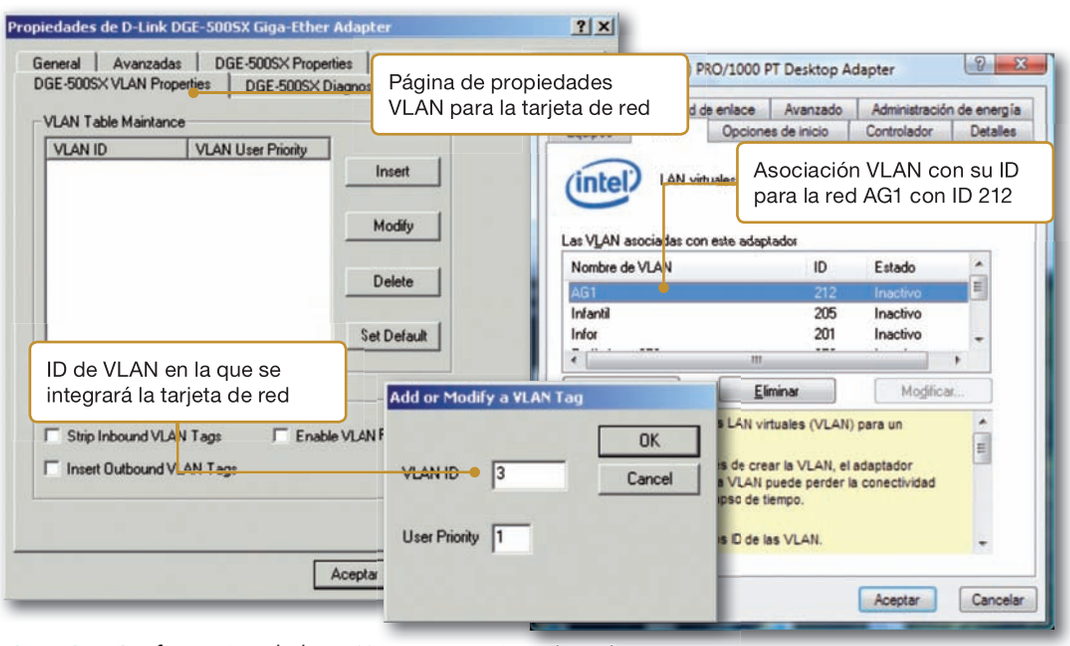


Fig. 5.21. *Configuración de la VLAN en una tarjeta de red.*

Actividades

8. En la instalación de red de una oficina bancaria trabajan varias decenas de empleados distribuidos en departamentos. Los oficinistas del departamento financiero tienen acceso a unos datos restringidos a los que no tienen acceso el resto de empleados. Todos deben tener derecho de uso de alguna impresora. El director de la oficina bancaria tiene que poder acceder a todos los datos locales de la sucursal. En el diseño de la red, los datos residen en uno o más servidores. Todos los usuarios se conectan a sus respectivas rosetas y no pueden cambiarse de roseta, ¿puede solucionar el problema de la privacidad una fragmentación de la red de tipo VLAN?, ¿la VLAN que propondrías asociaría las estaciones por puertos o por direcciones MAC? Si instalaras una VLAN por puertos, ¿ves más conveniente una solución Tag o Untag? Razona la respuesta.

9. Sobre la instalación del ejercicio anterior, ¿cómo solucionarías que el director de la oficina bancaria pueda acceder a todos los datos de la red?, ¿cómo tendría que ser configurado el puerto y la tarjeta de red de la impresora para que todos los usuarios pudieran acceder a ella? Por último, debate qué sería mejor: ¿una solución de un único servidor o una solución de varios servidores (uno por cada VLAN)? ¿Podría ser una solución aceptable instalar en el servidor múltiples tarjetas de red, cada una de las cuales estaría configurada en una VLAN?

Caso práctico 2

Construye una VLAN que proteja los segmentos de red

En el ejercicio profesional es muy común tener que hacer un despliegue de la red en donde con los mismos conmutadores se tengan que organizar varias redes locales, cada una de ellas asociada a una VLAN concreta, de modo que solo los dispositivos de red que pertenezcan a la misma VLAN sean alcanzables, pasando el resto inadvertidos.

Un ejemplo podría ser construir una VLAN para el departamento comercial de una empresa de modo que solo el personal de este departamento pueda acceder a la información de su servidor corporativo, que también estaría en la misma VLAN. Además, todo el tráfico generado por los comerciales quedará aislado del tráfico del resto de los departamentos de la empresa.

Claves y consejos

Es posible que sea necesario instalar en los *switches* la configuración de fábrica con objeto de eliminar todas las restricciones procedentes de una anterior instalación.

Para entrenar esta destreza vamos a familiarizarnos con los procedimientos típicos de configuración de VLAN. Para la realización de este ejercicio vamos a necesitar los siguientes materiales:

- Cuatro PC compatibles con IEEE 801.Q en sus tarjetas de red y sistema operativo de red en funcionamiento: dos de ellos simularán estar en la red de los comerciales y los otros dos en el resto de la red corporativa.
- Dos *switches* que soporten IEEE 801.Q y que simularán distintas ubicaciones en las oficinas de la empresa.
- Latiguillos de red para las conexiones de los PC a los *switches*.

En primer lugar tendremos que conectar todos los PC a los *switches*, que deberán estar conectados entre sí, y comprobar que todos los ordenadores pueden comunicarse entre sí. Esto significa que debemos partir de una red local sin restricciones en donde hemos comprobado que la configuración de los sistemas operativos, las direcciones de red y los cables de red funcionan correctamente.

En la Fig. 5.22 puede verse un ejemplo de la topología de conexión que necesitamos.

Una vez que tengas todo el hardware conectado según lo indicado y funcionando, vamos a realizar varias actividades:

1. Configura todas las tarjetas de red de los nodos para que no utilicen IEEE 802.1Q (esto significa que utilizaremos VLAN por puertos). Ahora creamos en el *switch* A una VLAN por puertos en donde el identificador de VLAN (VLANID) sea «1» y se le asocian los puertos «1» y «2» del *switch* A en su modalidad *untagged* (red VLAN por puertos), creando la VLAN número «1» con esos dos puertos. Comprueba que los nodos 1 y 2 siguen comunicándose entre sí, pero que no tienen comunicación con el resto de los nodos. Si «1» y «2» son las estaciones de los comerciales, tienen comunicación entre sí, mientras que las demás estaciones no pueden tener acceso a ellos. Esto se mantiene así mientras que los comerciales estén conectados a esos puertos concretos que acabamos de configurar.

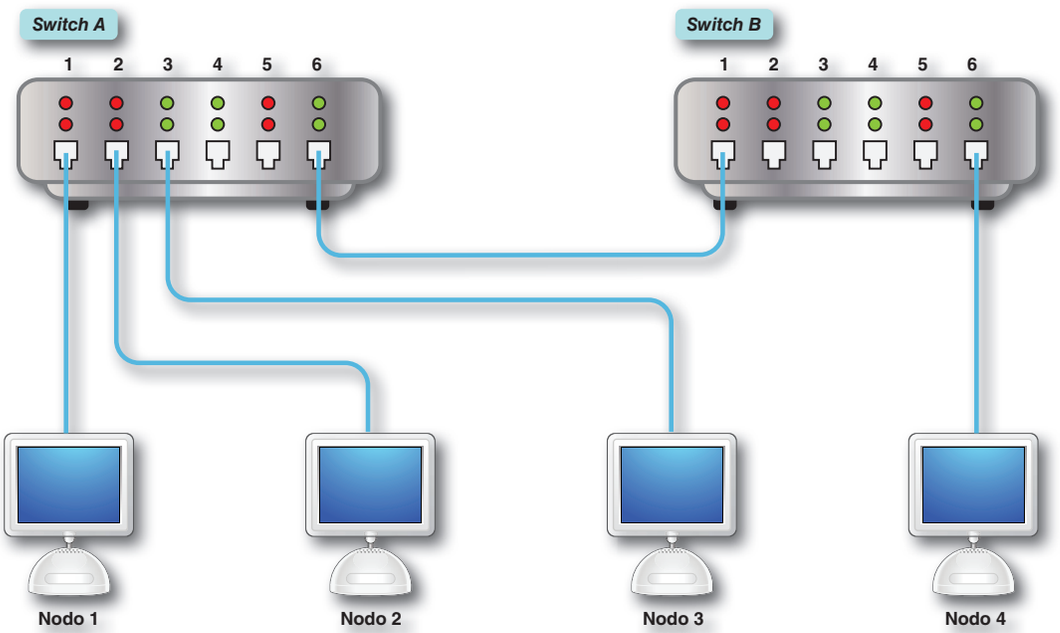


Fig. 5.22. *Topología de conexión para pruebas VLAN.*

Continúa...

Caso práctico 2

...Continuación

2. Ahora destruye la configuración anterior y habilita IEEE 801.Q en las tarjetas de red de los tres primeros nodos y en el *switch* A, es decir, ahora vamos a construir una VLAN no asociada a puertos. Asigna la VLANID 1 a la tarjeta de red del nodo 1, VLANID 2 al nodo 2 y VLANID 3 al nodo 3. Comprueba que, como los tres nodos pertenecen a tres VLAN distintas, no pueden comunicarse entre sí.

3. Seguidamente configura la tarjeta de red del nodo 3 para que tenga la VLANID 1. Ahora el nodo 1 y el nodo 3 pertenecen a la misma VLAN y, por tanto, podrán comunicarse entre sí, pero ninguno de los dos lo podrá hacer con el nodo 2.

Compruébalo. Este podría ser el caso de la llegada de un nuevo comercial al departamento que tiene la estación «3». El usuario de la estación «2» ha cambiado de departamento y, por tanto, ya no podrá acceder a su antigua VLAN de comerciales.

4. Habilita IEEE 801.Q en el *switch* B y en el nodo 4 asignándole a su tarjeta de red también el VLANID 1. Ahora los nodos 1, 3 y 4 pertenecen a la VLAN «1» y pueden comunicarse entre sí a pesar de que están conectados en *switches* distintos con tal de que el puerto 6 del *switch* A y el 1 del *switch* B tengan habilitados también IEEE 802.1Q y estén conectados físicamente con el cable apropiado. Habrá que configurar estos dos puertos para que se transmitan las tramas correspondientes a las VLAN que vayan a comunicarse entre los dos *switches*, por tanto lo más apropiado es configurar estos dos puertos como Tag y asignarles a los dos todas las VLAN definidas en los *switches*, es decir, estos puertos de intercomunicación pertenecerán a todas las VLAN. Comprueba que los nodos 1, 3 y 4 pueden comunicarse entre sí y que, sin embargo, ninguno de ellos puede hacerlo con el nodo 2.

Observa cómo, sin cambiar la estructura física de la red, hemos sido capaces de mover a los usuarios en distintos entornos de red.

Truco

Hay que asegurarse de que ambos *switches* son compatibles con el protocolo GVRP y que lo tienen habilitado para que las VLAN puedan atravesar las fronteras de cada *switch*.

5.2. Enlaces entre conmutadores

En las instalaciones reales es habitual tener que utilizar más de un conmutador para dar servicio a todos los usuarios, bien porque el número de usuarios sea muy elevado y supera el número de puertos del *switch* o bien porque la red se extiende geográficamente por zonas a las que un único conmutador no podría llegar.

Los conmutadores se enlazan entre sí a través de unos segmentos de red que los unen y que transportan el tráfico entre ellos. Obviamente, como estos segmentos tienen sus dos extremos conectados a sendos conmutadores, no admiten estaciones añadidas. Esta es la razón por la que se les llama segmentos despoblados. Técnicamente, a un segmento que une dos conmutadores se le denomina ***uplink.***

Además, como los conmutadores pueden tener configuradas varias VLAN, el *uplink* tendría que pertenecer a todas ellas, por lo que los puertos de un *uplink* deben estar configurados como Tag si los conmutadores quieren comunicar varias VLAN.

En la Fig. 5.22, el enlace *uplink* sería el segmento que une el puerto 6 del conmutador A con el puerto 1 del conmutador B.

Cuando el tráfico de la red entre *switches* es muy intenso es posible que un único *uplink* no tenga suficiente capacidad para mover las tramas de un conmutador a otro con la suficiente calidad de servicio. El administrador de la red puede agregar varios *uplink* y configurarlos como si fueran uno solo de mayor capacidad (agregación de enlaces, Fig. 5.23). A este agregado de enlaces se le llama **troncal** o ***trunk.***

La agregación de enlaces sigue la normativa **IEEE 802.3ad.** Frecuentemente *uplink* y troncal se toman como sinónimos obviando si es un agregado de enlaces o solo uno, pero un troncal suele llevar asociado el transporte de VLAN entre conmutadores.

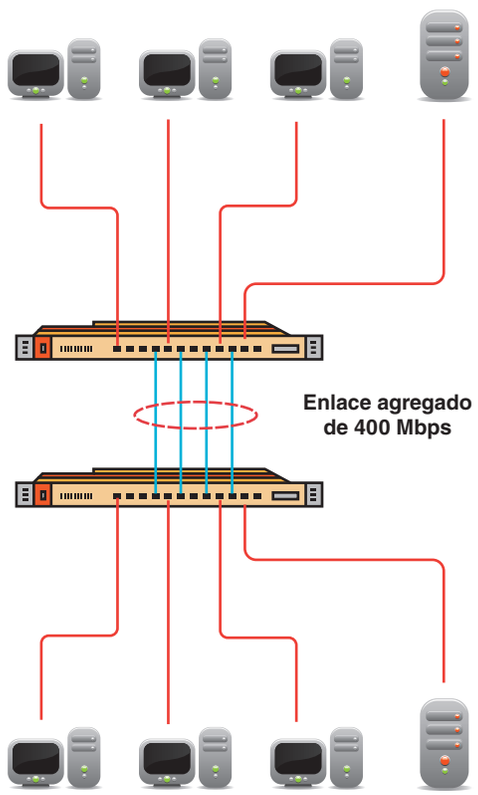


Fig. 5.23. *Enlace agregado de conexión entre dos conmutadores.*

Ampliación

Cuando un conmutador tiene que averiguar por qué puerto puede alcanzar un destino genera una trama de broadcast contra ese destino que emite por todos sus puertos de modo que a ese nodo de destino le llegue la trama con seguridad (si está activo) y conteste al *switch*. El conmutador aprenderá por qué puerto le llega la respuesta y utilizará ese puerto para transmitir las tramas con destino en ese nodo.

Las tramas de broadcast se transmiten por todos los puertos y pueden traspasar las fronteras entre *switches* (no así las de enrutadores, que no generan tramas de broadcast). Si las interconexiones entre *switches* forman bucles, estos pueden propagar las tramas de broadcast por estos bucles, repitiendo una y otra vez la información que transmiten, consumiendo inútilmente el ancho de banda de la red hasta el punto de que pueden llegar a inutilizarla por un consumo exhaustivo de los recursos disponibles. En este caso, se dice que se ha producido una **tormenta de broadcast.**

5.3. Tratamiento de bucles en la red: protocolos de *spanning tree*

Cuando la topología global de la red se hace compleja es posible que se formen bucles en la red, ya que una trama puede alcanzar su destino por varios caminos. Estas situaciones son muy interesantes porque proveen redundancia de caminos, lo que hace a la red menos sensible frente a averías en el sistema de cableado, pero también son una fuente de problemas puesto que se pueden generar tormentas de broadcast.

Por un lado, hay una necesidad de bucles para que haya redundancia pero, por otro lado, hay que impedir que se produzcan tormentas de broadcast. Para conseguir esto la IEEE ha propuesto un protocolo que impide los bucles en un nivel lógico, evitando las **tormentas de broadcast,** pero que reconfigura la red cuando algún segmento falla para utilizar las ventajas de la redundancia de segmentos físicos. Se trata del protocolo **IEEE 802.1D** o **STP** (*Spanning Tree Protocol,* Protocolo de árbol de expansión).

A. Características del protocolo STP

STP es un protocolo de nivel 2 diseñado originalmente para evitar tormentas de broadcast en redes conmutadas debido a la creación de bucles entre sus enlaces físicos.

Opera calculando los caminos de red que puedan evitar bucles y para ello bloquea artificialmente los enlaces que formarían un bucle entre cualquier origen y cualquier destino en la red conmutada.

STP se adapta dinámicamente a la topología de la red, de modo que si esta cambia, STP recalculará todos los posibles bucles y generará unos nuevos caminos exentos de bucles.

El modo de operación de STP en una red con conmutadores que incorporan esta tecnología y que además la tienen habilitada es el siguiente:

1. Se selecciona un conmutador determinado (*root bridge,* en la terminología de STP) y a partir de él se construye un árbol de caminos a cualquier otro conmutador (o *bridge*) de la red.
2. Se bloquean a nivel lógico los caminos que aparecen como redundantes entre cualesquiera origen y destino y se eligen como idóneos los que se calculan como más cortos.
3. Por estos caminos cortos circularán todas las tramas. Los puertos bloqueados no podrán transferir tramas de datos entre las estaciones, solo pueden transmitir las tramas de control del propio protocolo STP.
4. Si uno de los caminos más cortos falla (por ejemplo, se ha deteriorado el cable de red que lo soporta), se recalcula el árbol de caminos para hallar un nuevo camino que obvie el fallo. Este proceso consume un tiempo durante el que la red no estará operativa (tiempo de convergencia de STP). Este tiempo dependerá de la complejidad de la red, pero puede superar el minuto, lo que a veces puede ser inaceptable.

Para mejorar el tiempo de convergencia se han creado protocolos más modernos, derivados del STP que reducen significativamente el tiempo de convergencia a unos pocos segundos. Un ejemplo de estos nuevos protocolos es **RSTP** *(Rapid Spanning Tree Protocol),* que está recogido en la norma **IEEE 802.1w.**

B. Operación con el protoolo STP

En la Fig. 5.24 se puede ver la representación gráfica de una red conmutada con tres *switches* con caminos redundantes que será útil para estudiar el modo de operación básica de STP. Efectivamente, para que una trama con origen en PC1 llegue a PC3, caben dos caminos: el camino más sencillo consiste en enviar la trama por el camino 2 hacia el conmutador C y él se encargará de conducirla hacia su destino en PC3. El segundo camino tiene un mayor coste y consiste en transmitir la trama por el camino 1 hacia el conmutador B y que este redirija la trama por el camino 3 hacia el conmutador C que es quien tiene la conexión física con el destino PC3.

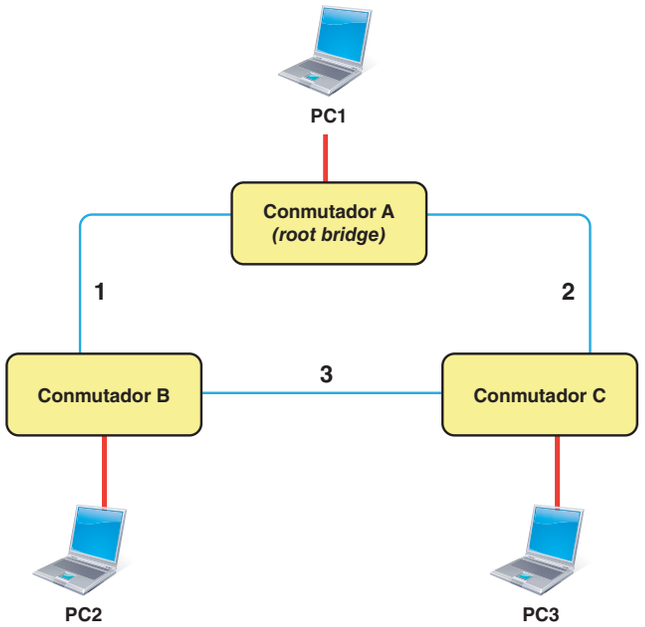


Fig. 5.24. *Ejemplo de redundancia de caminos en una red conmutada para el estudio del protocolo STP.*

La red reúne todos los elementos para que se genere una tormenta de broadcast puesto que tiene bucles. Por ello, es necesario habilitar en los tres conmutadores el protocolo STP o RSTP. Una vez habilitados los conmutadores negociarán quién debe tomar la función de *root bridge*. Supongamos que esta función sea asumida por el conmutador A, como aparece en la figura.

Una vez que haya convergido el proceso de confección del árbol de caminos de STP, el protocolo habrá decidido anular el camino 3. Esto no quiere decir que haya que quitar el latiguillo de conexión de este segmento, sencillamente, STP anulará ese camino impidiendo que por él pasen tramas de datos.

De este modo, PC1 podrá comunicar con PC2 a través el camino 1, PC1 podrá comunicarse con PC3 mediante el camino 2, mientras que PC2 se comunicará con PC3 utilizando los caminos 1 y 2 a través del conmutador A.

Si en un momento dado el camino 1 deja de estar disponible, entonces quedarán incomunicadas todas las estaciones que tienen que utilizar este camino 1 en sus comunicaciones. STP se da cuenta del fallo de red y genera un nuevo árbol anulando el camino 1.

En este caso, STP elegirá los caminos 2 y 3 para asegurar sus comunicaciones y así, PC1 podrá comunicarse con PC3 a través del camino 2, PC2 se comunicará con PC3 por el camino 3 y PC1 lo hará con PC2 a través de los caminos 2 y 3.

Por tanto, STP ha sido capaz de utilizar la redundancia física de la topología de la red, impidiendo que se formen bucles lógicos que causen tormentas de broadcast.

Actividades

10. Sobre el ejemplo de red conmutada representada en la Fig. 5.24, ¿cuáles serían los caminos que elegirían los conmutadores para transmitir tramas entre las tres estaciones suponiendo que fallara el *uplink* del camino 2? ¿Y si fallan los caminos 2 y 3?

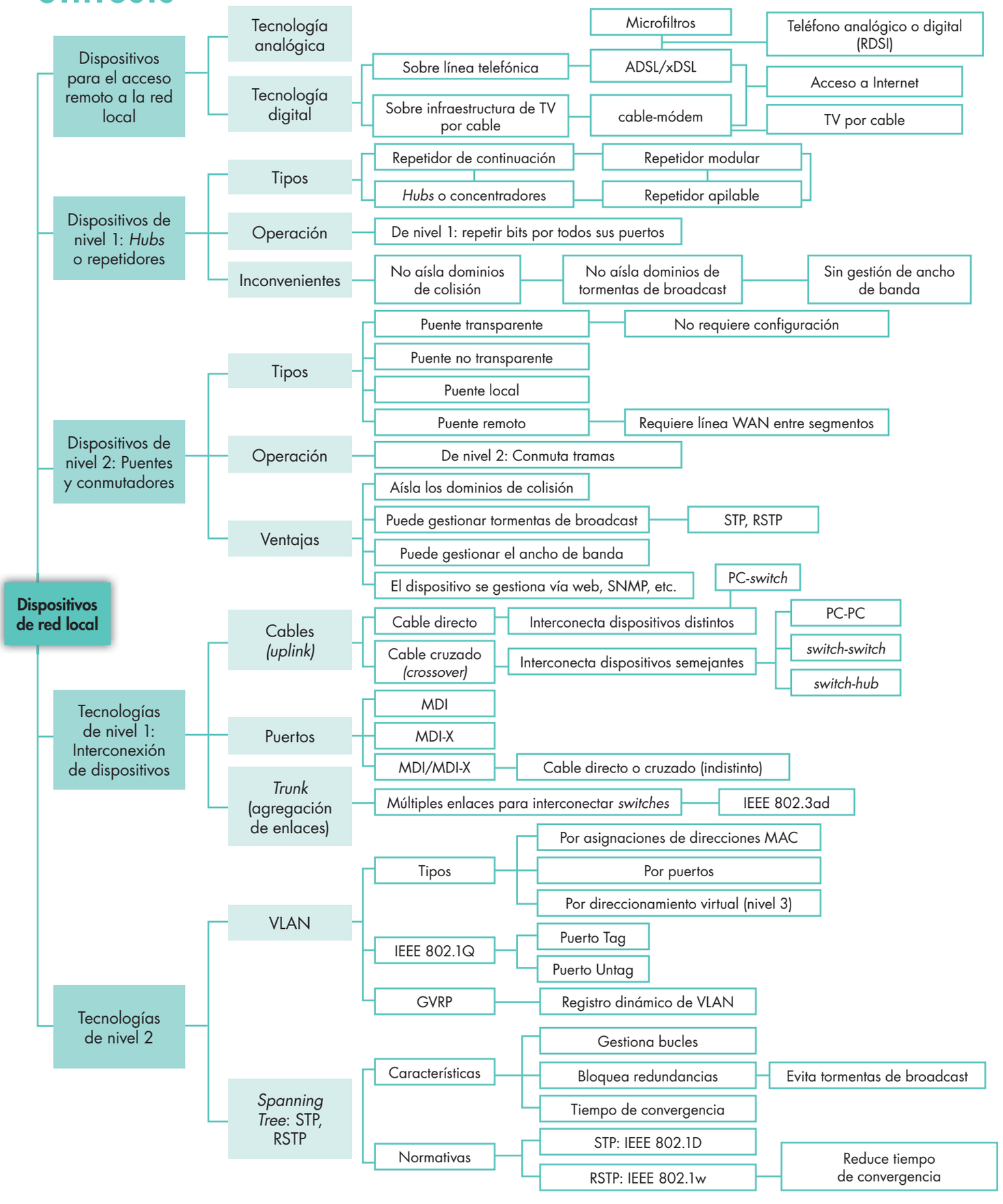
Investigación

Los conmutadores son en la actualidad los dispositivos más utilizados para realizar el despliegue de la red: repetidores y concentradores solo se utilizan en casos muy específicos y siempre minoritarios. Los *switches* incorporan muchas otras funciones además de la conmutación de tramas que es en la que se especializan.

Puedes investigar algunos ejemplos de estas tecnologías en Wikipedia por la voz «switch» y, más en concreto, en la tecnología «spanning tree» que se encarga de resolver conflictos de tramas que pueden entrar en un bucle cuando la topología de red es mucho más complicada que una simple estrella y forma bucles entre sus segmentos. El protocolo original fue STP *(Spanning Tree Protocol)*, que producía paradas en el servicio de red durante decenas de segundos cuando se alteraba la topología de la red, aunque actualmente se utiliza mucho más RSTP *(Rapid Spanning Tree Protocol)*, que gestiona mucho más rápidamente los cambios topológicos de los segmentos de red.

En las páginas **http://es.wikipedia.org/wiki/Spanning_tree** y **http://es.wikipedia.org/wiki/Rapid_Spanning_Tree_Protocol** dispones de una buena información para comenzar el estudio de STP y RSTP respectivamente.

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de algunas de las tecnologías de bajo nivel, básicas en el acceso remoto a la red:

a) ADSL	1) Cableado telefónico
b) Cable-módem	2) La velocidad de bajada es distinta de la de subida
	3) Televisión por cable
	4) Instalación de microfiltros

2. El *hub* o repetidor…

a) Opera en el nivel 2 de OSI.

b) Opera en el nivel 3 de OSI.

c) Opera en el nivel 1 de OSI.

d) Opera en los niveles 1 o 2, dependiendo de su configuración.

3. Asocia las siguientes tecnologías específicas de los conmutadores a sus normativas específicas:

a) VLAN	1) IEEE 802.1D
b) STP	2) IEEE 802.1w
c) RSTP	3) IEEE 802.1Q
d) Trunking	4) IEEE 802.3ad

4. Los conmutadores…

a) Son multipuerto.

b) Intercambian paquetes entre sus puertos.

c) Intercambian tramas entre sus puertos.

d) Fraccionan los dominios de colisión.

5. Asocia las características de *hubs* y conmutadores:

a) *Hub*	1) Puente
b) *Switch*	2) Repetidor
	3) Nivel 2
	4) Nivel 1
	5) Conmutador
	6) Conmuta tramas
	7) Interpreta las cabeceras de las tramas
	8) No discrimina las tramas

6. ¿Qué función de las siguientes no es específica de los conmutadores de nivel 2?

a) Conmutar tramas entre sus puertos.

b) Convertir tramas Ethernet en tramas Token ring.

c) Crear redes locales virtuales.

d) Encaminar paquetes.

7. Un *root bridge* es:

a) El nodo raíz de una VLAN.

b) El nodo raíz de un árbol STP.

c) La estación conectada a un conmutador que tiene habilitado STP.

d) Un conmutador redundante.

8. Enlaza los elementos de las columnas en la tabla siguiente sobre el estado de los puertos de un conmutador que utiliza la tecnología IEEE 802.1Q:

a) Puerto Tag	1) Admite tramas Ethernet no modificadas con la información de VLAN
b) Puerto Untag	2) Admite tramas Ethernet modificadas con la información de VLAN
	3) El conmutador gestiona la modificación de la trama con la información de VLAN
	4) El conmutador conmuta la trama sin modificarla

9. Una tormenta de broadcast:

a) Puede agotar los recursos de la red.

b) Se genera por la transmisión redundante de paquetes de nivel 3 en la red.

c) Se genera por la transmisión redundante de tramas de nivel 2 por todos los puertos de la red.

d) Se puede gestionar mediante el protocolo RSTP.

10. Dos conmutadores tienen definidas las dos mismas VLAN en cada uno de ellos. Se desea transmitir tramas de uno a otro a través de enlaces entre ellos. Determina cuál de las siguientes afirmaciones es verdadera.

a) Basta un enlace *(uplink)* entre dos puertos de sendos conmutadores (uno por cada conmutador) sin ninguna configuración posterior.

b) Basta un enlace *(uplink)* entre dos puertos de sendos conmutadores (uno por cada conmutador), pero hay que configurar que estos dos puertos pertenezcan a las dos VLAN en cada uno de los dos conmutadores.

c) Hay que crear un *trunking* con dos puertos en cada conmutador.

d) El enlace de conexión entre los conmutadores debe ser Tag en un extremo y Untag en el otro.

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

Comprueba tu aprendizaje

I. Distinguir las funciones de los dispositivos de interconexión de red

1. Confirma la veracidad o falsedad de las siguientes afirmaciones:

   a) Externamente, un *hub* y un *switch* se distinguen con dificultad.

   b) Un puente remoto consta de dos dispositivos separados por una línea de conexión.

   c) Los conmutadores operan en el nivel 3 y los puentes en el nivel 2.

   d) Los repetidores se pueden instalar en cascada indefinidamente.

   e) Los conmutadores saben gestionar el ancho de banda de cada puerto.

   f) Los repetidores y concentradores copian las tramas entre sus puertos.

2. Relaciona la columna de la izquierda (dispositivos) con su tecnología específica (columna de la derecha). Ten en cuenta que la relación es de uno a varios.

Dispositivos	Tecnología o función específica
1. Repetidor	a. Conmutar paquetes
2. *Transceiver*	b. Regenerar la señal eléctrica
3. Concentrador	c. Doble puerto
4. Puente	d. Múltiple puerto
5. *Switch*	e. Selecciona tramas

3. ¿Es posible crear VLAN utilizando conmutadores? ¿Y si utilizamos concentradores? ¿Y si usamos puentes remotos?

II. Elegir los dispositivos de red de área local en función de las necesidades

4. Busca los errores técnicos en el siguiente comentario:

   «Una empresa acaba de fusionarse con otra y sus directivos proyectan integrar sus dos redes antiguas en una nueva. Cada red está en la sede de su ciudad original. Se ha propuesto la adquisición de un puente remoto para unir las dos sedes, pero una vez comprobado su escaso rendimiento se ha determinado conectarlas mediante un conmutador que es mucho más rápido.»

5. Confirma la veracidad o falsedad de las declaraciones siguientes sobre ADSL:

   a) La tecnología xDSL siempre es simétrica.

   b) En ADSL el ancho de banda de bajada suele ser superior al de subida porque es una tecnología asimétrica.

   c) Un módem ADSL siempre requiere otro dispositivo intermedio para conectarse a la red local.

   d) Al igual que el módem, el router ADSL también requiere un dispositivo intermedio para unirse a la red.

6. Busca en las sedes web de los fabricantes de dispositivos de red información técnica y comercial sobre conmutadores.

   Compara los distintos modelos de varios fabricantes para familiarizarte con las características básicas de este tipo de dispositivos.

   Si consigues listas de precios, podrías realizar comparativas de precios.

   Ayuda: Las comparativas de precios no se hacen por conmutador, sino por puertos, es decir, se divide el precio total del conmutador por el número de puertos que posee.

III. Configurar redes locales virtuales

7. ¿Qué tipos de redes de área local virtuales conoces? ¿Cómo se llama el estándar IEEE utilizado en la creación de VLAN?

8. Razona en qué condiciones podrían ser verdad las siguientes afirmaciones:

   a) Dos puertos que se asocian en la misma VLAN en un conmutador pueden comunicarse libremente.

   b) Dos puertos que pertenecen a dos VLAN distintas solo pueden comunicar los protocolos de gestión.

   c) Las direcciones MAC de los dos nodos se han asociado a la misma VLAN, pero como están conectados en dos conmutadores distintos, nunca podrían comunicarse entre sí.

   d) Dos nodos que pertenecen a la misma VLAN pero que están conectados a distintos conmutadores pueden comunicarse entre sí.

9. Toma tres conmutadores que contemplen el protocolo STP o RSTP y prepara en el laboratorio un modelo para la red conmutada que aparece en la Fig. 5.24.

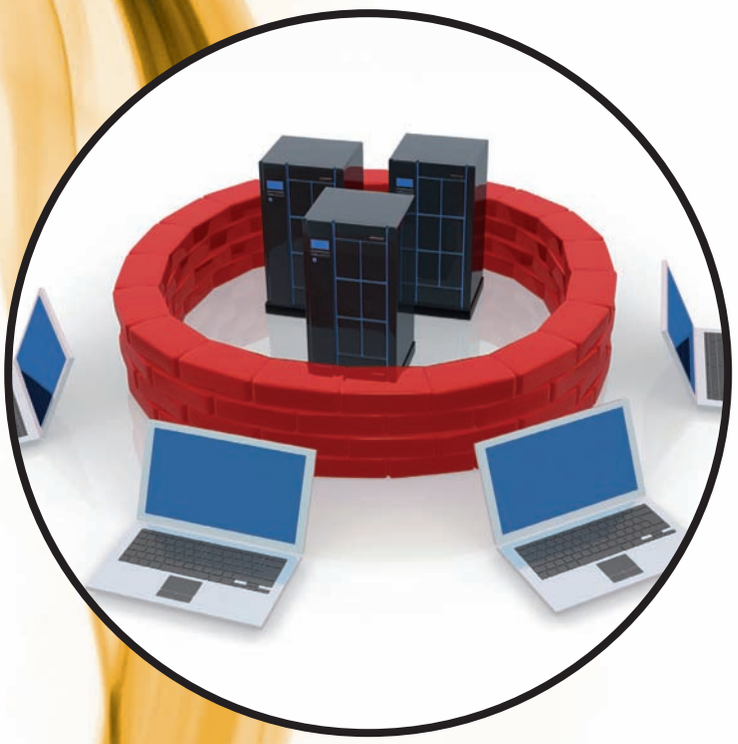
   a) Habilita el protocolo STP en los tres conmutadores y comprueba que las tres estaciones pueden comunicarse entre sí.

   b) Rompe ahora el enlace del camino 1 y comprueba que después de un tiempo sigues teniendo conexión entre las estaciones.

   c) Repite el proceso anterior deshabilitando los caminos 2 y 3.

Unidad 6

Interconexión de equipos y redes



En esta unidad aprenderemos a:

- Configurar los clientes de una red local para utilizar un sistema de enrutamiento.
- Gestionar un proxy web.
- Diseñar y configurar un sistema de protección para la red local.

Y estudiaremos:

- Los protocolos de acceso desde y hacia la red WAN externa.
- Los parámetros de configuración en enrutadores y servidores proxy.
- La tecnología de una red perimetral.
- Las órdenes que permiten crear y modificar las tablas de rutas de nodos y encaminadores.

CEO

SMR_RL_AAbad_06_TramaPPP.docx

Documento que contiene información sobre el formato de la trama PPP.

Vocabulario

Encapsulación de protocolo: encapsular un protocolo A dentro de otro B es ponerle cabeceras de protocolo B a cada paquete de datos del protocolo A. Como ejemplo, podríamos decir que el transporte ferroviario de coches consiste en encapsular según las normas ferroviarias el transporte habitual por carretera.

Frecuentemente se utiliza el término «tunelización» como sinónimo de encapsulación de un protocolo.

Investigación

PPPoE *(PPP over Ethernet)* es un protocolo derivado de PPP que se utiliza mucho para utilizar la tecnología PPP cuando la red de transporte es Ethernet. Busca información en Internet sobre el protocolo para descubrir dónde radican sus ventajas.

Puedes empezar tu búsqueda por **http://www.adslzone.net/adsl_pppoe.html** y por la voz PPPoE en Wikipedia.

De modo análogo también hay un protocolo PPPoA (PPP over ATM), que es semejante a PPPoE pero sustituye Ethernet por una red ATM.

Otras direcciones de interés son: **http://es.wikipedia.org/wiki/PPPoA , http://es.wikipedia.org/wiki/PPPoE** y **http://www.adslfaqs.com.ar/que-es-el-pppoe-y-pppoa-explicacion-sencilla/**

1. El acceso a las redes WAN

Los ordenadores no son entidades aisladas, y las redes tampoco. De igual modo que los ordenadores se relacionan entre sí utilizando redes de área local, estas pueden interconectarse mediante otras redes de ámbito mayor: las redes de área extensa.

A menudo se segmenta la red de área local corporativa creando varias subredes e interconectándolas entre sí utilizando dispositivos específicos de los que nos ocuparemos en esta unidad.

Las redes WAN no suelen conectar directamente nodos, sino que interconectan redes. Lo específico de ellas es que las líneas que suelen utilizar son públicas y los protocolos de comunicación que requieren tener en cuenta la seguridad de un modo especial.

1.1. Protocolos de acceso remoto

La importancia que tenía el adaptador de red y los protocolos de nivel uno y dos para las redes de área local la tienen ahora los protocolos de acceso remoto para las redes WAN.

A. Protocolo PPP

Bajo la denominación PPP (*Point to Point Protocol*, protocolo punto a punto) se designa a un conjunto de protocolos que permiten el acceso remoto para el intercambio de tramas y autenticaciones en un entorno de red de múltiples fabricantes. Un cliente PPP puede efectuar llamadas y, por tanto, establecer conexiones a cualquier servidor que cumpla las especificaciones PPP. La arquitectura PPP permite que los clientes puedan ejecutar cualquier combinación de los protocolos NetBeui, IPX y TCP/IP, incluyendo las interfaces NetBIOS y sockets de red.

Aunque tradicionalmente PPP ha sido utilizado en conexiones sobre líneas serie, por ejemplo: para marcar por módem y realizar una conexión a Internet, existe una versión en la que se encapsula PPP sobre una capa Ethernet denominada PPPoE *(PPP over Ethernet)*, ampliamente utilizada para proveer conexiones de banda ancha añadiendo a Ethernet las ventajas que PPP ofrece como autenticación, cifrado y compresión de datos.

B. Protocolo SLIP

SLIP (*Serial Line Internet Protocol*, protocolo Internet para línea serie) es un protocolo estándar utilizado desde hace tiempo en sistemas UNIX que permite la conexión remota a través de líneas serie utilizando el protocolo IP. Los servidores de acceso remoto siguen contemplando el protocolo SLIP por compatibilidad, aunque está siendo desplazado por PPP.

C. El protocolo de tunelización PPTP

PPTP (*Point to Point Transport Protocol*, protocolo de transporte punto a punto) es un protocolo que encapsula los paquetes procedentes de las redes de área local de modo que se hacen transparentes a los procedimientos de red utilizados en las redes de transporte de datos.

El protocolo PPTP está definido en el RFC 2637. Sus comunicaciones son cifradas y es bastante popular en redes privadas virtuales, que estudiaremos más adelante, ya que Microsoft incorporó un servidor y un cliente PPTP a partir de Windows NT, algo también común en el mundo Linux.

Por ejemplo, dos redes IPX pueden crear un túnel PPTP a través de Internet, de modo que se crea una red virtual utilizando Internet (red IP) como medio de transporte, pero intercambiándose paquetes IPX transparentemente.

1.2. Servicios de acceso remoto

El servicio de acceso remoto *(RAS, Remote Access Service)* conecta equipos remotos, posiblemente móviles, con redes corporativas, es decir, permite las conexiones de equipos distantes de la red de área local, habilitando los mismos servicios para estos usuarios remotos que los que poseen los usuarios presentados localmente. Por tanto, RAS es un encaminador software multiprotocolo con capacidad de autenticación y encriptación de los datos transmitidos.

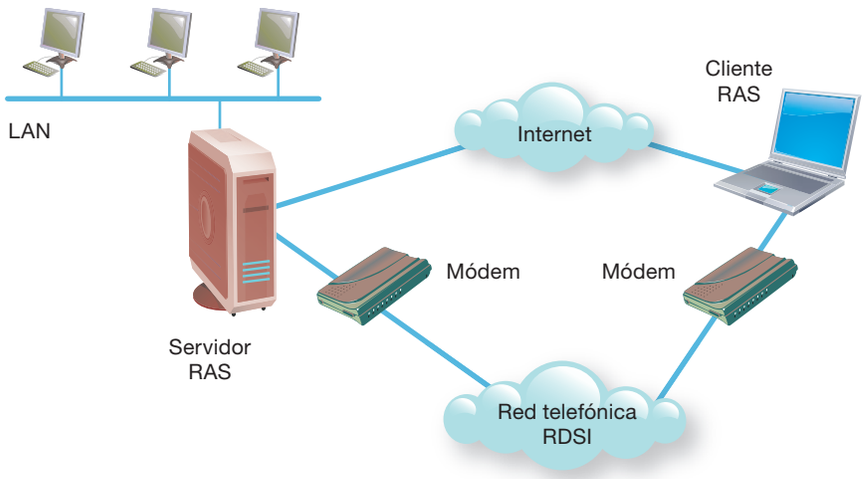


Fig. 6.1. *Esquema del acceso de una estación cliente a un servidor RAS y a su red de área local.*

A. Escenario de conexión RAS

El servicio de acceso remoto tiene una parte de cliente (quien se conecta) y otra de servidor (lugar al que se conecta el cliente). Son posibles conexiones punto a punto a través de módems analógicos, redes X.25, RDSI, ADSL e incluso RS-232-C. Además, es posible la conexión entre el cliente y el servidor a través de Internet de modo transparente a la red, utilizando el protocolo de túnel PPTP.

RAS es capaz de encaminar tres protocolos de LAN: IPX, TCP/IP y NetBeui, ya que frecuentemente utiliza PPP como transporte y este puede encapsular los tres protocolos de LAN. Por tanto, cualquier cliente que utiliza al menos alguno de estos tres protocolos puede realizar una conexión vía RAS hacia una red que ejecute estos mismos protocolos. Es posible configurar el servicio RAS para que el cliente tenga acceso a toda la red o exclusivamente al servidor RAS.

Cuando el cliente se conecta a través de NetBeui, apenas hay nada que configurar, puesto que NetBeui es un protocolo para redes planas cuyo único elemento de configuración es el nombre NetBIOS.

Si un cliente RAS se conecta vía TCP/IP, necesitará una dirección IP compatible con la red a la que intenta conectarse. Lo normal es que el servidor RAS le asigne dinámicamente una dirección que utilizará mientras dure la conexión. Esta es la razón por la que frecuentemente los servidores de acceso remoto incluyen un servidor DHCP o se integran con el DHCP corporativo.

Para el cliente RAS, todo el procedimiento de red es transparente. A través de las interfaces de red apropiadas como NetBIOS o sockets, sus aplicaciones de red funcionarán perfectamente desde su posición remota como si estuvieran en la misma red de área local.

Ampliación

En las versiones recientes de los servidores Windows, Microsoft ha mejorado aún más el servicio de acceso remoto y lo ha denominado RRAS (*Routing and Remote Access Service*, Servicio de enrutamiento y acceso remoto). Puede conseguirse más información sobre RRAS en **http://technet.microsoft.com/es-es/network/bb545655**

Actividades

1. Confirma la veracidad de las siguientes afirmaciones:
   a) El protocolo PPP puede gestionar intercambio de paquetes de cualquier protocolo de red.
   b) PPTP es un protocolo que crea túneles sobre los que se encapsula TCP/IP, NetBeui o SPX/IPX.
   c) Un protocolo de gestión de la autenticación es el que se encarga de pedir el nombre de usuario y su contraseña.
   d) Basta con incorporar a la comunicación cualquier protocolo de autenticación para que la comunicación sea totalmente segura.
2. Descubre el error en el siguiente razonamiento: «El administrador de red de una instalación ha preparado un sistema Linux en el portátil de un comercial que estará de viaje. Desde ese portátil el comercial hará conexiones remotas hacia un servidor RAS Windows localizado en la sede central de las oficinas. El servidor solo tiene configurado el protocolo NetBeui de Microsoft. Cuando el portátil, que tiene Linux, se conecta al servidor RAS emplea el protocolo PPP para transportar paquetes TCP/IP al servidor RAS. Como RAS es compatible con TCP/IP y NetBeui, no importa que cliente y servidor "hablen" protocolos distintos: el sistema hace transparente la comunicación al usuario.»

CEO

SMR_RL_AAbad_06_TecnologiasRedesWAN.docx

Documento que contiene información sobre:

1. Ejemplo de secuencia de conexión con RAS.
2. Gestión multienlace.
3. Canales para redes WAN.

2. El encaminador

Los encaminadores, enrutadores o routers son dispositivos software o hardware que se pueden configurar para encaminar paquetes entre sus distintos puertos de red utilizando la dirección lógica correspondiente a la Internet (subred), por ejemplo, su dirección IP.

Puesto que la función de encaminamiento se realiza de acuerdo con reglas formadas con las direcciones de red (nivel 3), solo serán enrutables aquellos protocolos que participen de este nivel. Por ejemplo, puesto que la familia de protocolos que utiliza NetBIOS de modo nativo no tiene la capa 3 (no hay direcciones de red NetBIOS), se puede deducir que NetBIOS no es encaminable: solo funcionará en redes locales y no podrá saltar a otras redes.

2.1. Características generales

El encaminador interconecta redes de área local operando en el nivel 3 de OSI (Fig. 6.2). El rendimiento de los enrutadores es menor que el de los conmutadores ya que deben gastar tiempo del proceso en analizar los paquetes del nivel de red que le llegan. Sin embargo, permiten una organización muy flexible de la interconexión de las redes.

Claves y consejos

La configuración de los encaminadores puede llegar a ser una de las tareas más difíciles del administrador de red, especialmente en redes complejas y en donde los caminos no son únicos. Las compañías fabricantes de routers suelen ofrecer a sus clientes formación específica en cada uno de sus productos. En cualquier caso, constituye un buen hábito laboral tener el manual del fabricante cerca cuando se configuran estos dispositivos.

Cada enrutador encamina uno o más protocolos. La condición que debe imponerse al protocolo es que sea enrutable, porque no todo protocolo se puede encaminar. Los routers comerciales suelen tener capacidad para encaminar los protocolos más utilizados, todos ellos de nivel 3: IP, IPX, AppleTalk, DECnet, XNS, etc.

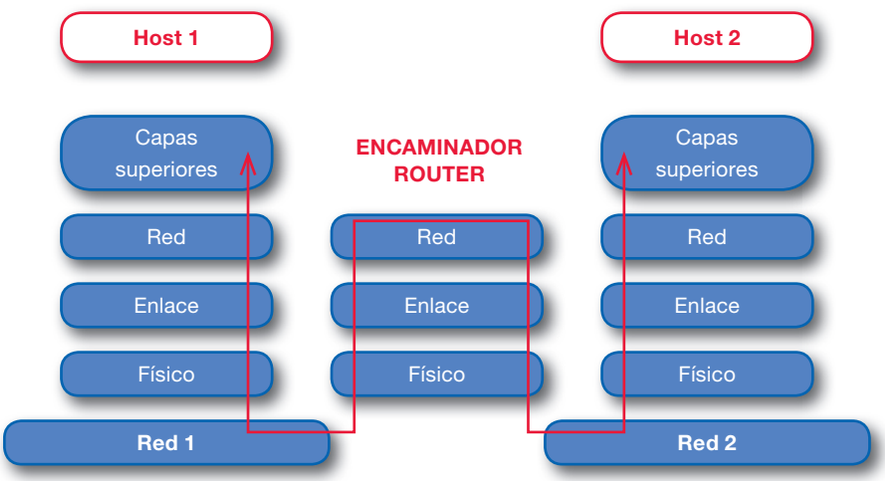


Fig. 6.2. *Esquema de operación en la arquitectura de red de un encaminador.*

Las características fundamentales de los encaminadores se pueden resumir en que:

- Interpretan las direcciones lógicas de capa 3, en vez de las direcciones MAC de capa de enlace, como hacen los puentes o los conmutadores.
- Son capaces de cambiar el formato de la trama, ya que operan en un nivel superior a la misma.
- Poseen un elevado nivel de inteligencia y pueden manejar distintos protocolos previamente establecidos.
- Proporcionan seguridad a la red puesto que se pueden configurar para restringir los accesos a esta mediante filtrado.
- Reducen la congestión de la red aislando el tráfico y los dominios de colisión en las distintas subredes que interconectan. Por ejemplo, un router TCP/IP puede filtrar los paquetes que le llegan utilizando las máscaras IP.

A. Tipos de encaminadores

Pueden establecerse diversas clasificaciones de los encaminadores en función del aspecto que se ponga en estudio, pero los más comunes atienden al lugar en donde se ubican y al protocolo de enrutamiento que utilizan.

A.1. Según su ubicación en la red

Es frecuente que los routers se clasifiquen de acuerdo con el ámbito de la red a la que proporcionan servicio. Según esto, un encaminador puede ser:

- **Router de interior** *(Interior router).* Se trata de un encaminador para ser instalado en una LAN para dar servicio de encaminamiento dentro de la propia red de área local proporcionando a los paquetes de red la posibilidad de saltar de unos segmentos de la red a otros.
- **Router de exterior** *(Exterior router):* en este caso el encaminador comunica nodos y redes en el exterior de la LAN. Estos routers operan típicamente en el núcleo de Internet y son utilizados por los operadores de Internet para comunicarse entre ellos.
- **Router de borde o frontera** *(Gateway router o Border router).* Es un encaminador que se encarga de conectar routers interiores con routers exteriores. Por ejemplo, pueden intereconectar una LAN a Internet a través del proveedor de servicios de Internet (ISP, *Internet Service Provider*).

A.2. Según el tipo de algoritmo de encaminamiento

Los routers confeccionan una tabla de encaminamiento en donde registran qué nodos y redes son alcanzables por cada uno de sus puertos. Es decir, la tabla describe la topología de la red. De aquí nace una segunda clasificación de los algoritmos utilizados por los encaminadores para realizar su función:

- Algoritmos de **encaminamiento estático** *(static routing).* Requieren que la tabla de encaminamiento sea programada por el administrador de red. Carecen de capacidad para aprender la topología de la red por sí mismos, cualquier adaptación a cambios topológicos de la red requiere una intervención manual del administrador del router.
- Algoritmos de **encaminamiento adaptativo** *(dynamic routing).* Son capaces de aprender por sí mismos la topología de la red. Por tanto, son mucho más flexibles que los encaminadores estáticos, aunque su rendimiento es menor puesto que tienen que consumir recursos en el intercambio de información con otros enrutadores para, dinámicamente, confeccionar las tablas de encaminamiento que contienen la información con la que tomará las decisiones de enrutamiento de paquetes.

Fig. 6.3. *Algunos modelos de encaminadores. Cisco es una de las compañías líderes en ventas de enrutadores.*

Claves y consejos

No hay que confundir protocolo enrutable con protocolo de enrutamiento. Un protocolo enrutable es aquel que proporciona paquetes al router para que este los encamine hacia su destino. Un protocolo de enrutamiento es el protocolo que utiliza el router para comunicarse con otros routers y aprender la topología de la red.

B. Protocolos de encaminamiento

Un protocolo de encaminamiento es aquel que utiliza un router para calcular el **mejor camino** (*best path,* en la terminología profesional) que le separa de un destino determinado. El mejor camino calculado representa la ruta más eficiente que debe seguir un paquete desde que sale de un nodo origen hasta que llega a su destino pasando por el router.

El mejor camino dependerá de la actividad de la red, de si hay enlaces fuera de servicio, de la velocidad de transmisión de los enlaces, de la topología de la red y de muchos otros factores. Así, un enlace de alta velocidad representará un camino mejor que otro semejante pero de menor velocidad.

El **coste de una ruta** *(route cost)* es un valor numérico que representa cuán bueno es el camino que la representa: a menor coste, mejor camino.

Un protocolo de enrutamiento se caracteriza también por su **tiempo de convergencia,** que es el tiempo que tarda un router en encontrar el mejor camino cuando se produce una alteración topológica en la red que exige que se recalculen las rutas para adaptarse a la nueva situación. Hay que diseñar los protocolos de enrutamiento para que tengan el menor tiempo de convergencia posible.

De modo genérico, a los protocolos de enrutamiento utilizados con routers de interior se les denomina **IGP** *(Interior Gateway Protocol)* mientras que a los utilizados con routers de exterior se les denomina **EGP** *(Exterior Gateway Protocol).*

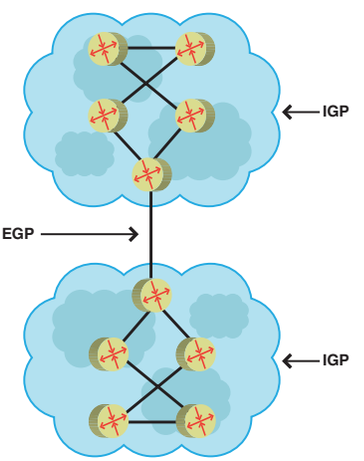


Fig. 6.4. *Lugares de la red en donde deben utilizarse protocolos IGP o EGP.*

B.1. Protocolos de enrutamiento basados en el vector-distancia

Un protocolo de encaminamiento basado en un vector-distancia es aquel que determina cuál es el mejor camino calculando la **distancia al destino.** La distancia es un número calculado que no necesariamente significa longitud, sino que puede contemplar otros parámetros como el número de saltos que dará para llegar al destino (número de routers por los que pasará el paquete en su viaje hacia su destino), la latencia (tiempo medio en llegar al destino) u otros valores que impliquen costes económicos en la transferencia del paquete que debe enrutarse.

Con vector-distancia, el router debe intercambiar periódicamente su información de enrutamiento con otros routers vecinos para recalcular las nuevas distancias entre ellos.

Los protocolos de enrutamiento basados en vector-distancia más utilizados actualmente son RIP, RIPv2 y BGP.

- **RIP** o **RIPv1** *(Routing Information Protocol)* es un algoritmo de tipo vector basado en la RFC 1058 apropiado para encaminamiento en redes IP pequeñas. Solo se utiliza en routers interiores y de borde. RIP utiliza cada 30 segundos el puerto UDP número 520 para intercambiar la información de encaminamiento con otros enrutadores, que se calcula como el cómputo de saltos de red necesarios para que un paquete dado alcance su destino. RIP no considera la congestión de la red ni la velocidad del enlace. Si la red es grande, RIP genera excesivo tráfico de red por lo que es muy poco escalable. Además, su convergencia es muy pobre. A cambio, es un protocolo muy estable y está implementado en la mayor parte de los enrutadores. Para que no forme bucles, RIP limita el número de saltos con otros enrutadores para intercambiar información a 15, por lo que si el destino se encuentra más lejos de 15 saltos, RIP considerará el destino como inalcanzable.
- **RIPv2** (*Routing Information Protocol* versión 2) es una actualización de RIPv1 que genera menos tráfico de *broadcast,* admite *subnetting* y mejora la seguridad pues en el intercambio de información de enrutamiento se emplean contraseñas. Sin embargo, sigue sin poder exceder los 15 saltos, por lo que sigue siendo poco escalable.
- **BGP** *(Border Gateway Protocol)* es un protocolo de frontera exterior, es decir, se ejecuta en los encaminadores que forman el perímetro de la red y facilitan extraordinariamente el intercambio de rutas con los encaminadores exteriores, típicamente propiedad de los proveedores de Internet. BGP utiliza el puerto TCP número 179 para intercambiar mensajes específicos. El administrador de la red puede configurar BGP para que siga unas políticas que determinen caminos preferentes.

B.2. Protocolos de enrutamiento basados en el estado del enlace

Un protocolo de encaminamiento basado en el estado del enlace *(link-state)* es aquel que le permite a un router crearse un mapa de la red para que él mismo pueda determinar el mejor camino a un destino por sí mismo examinando el mapa que se ha construido. En función de la información de los enlaces que mantiene con sus routers vecinos y la información que estos le proporcionen sobre los segmentos de la red que ellos ven, construirán árboles de caminos que representen el mapa de la red.

Los protocolos de enrutamiento basados en el estado del enlace más utilizados actualmente son OSPF e IS-IS.

- **OSPF** *(Open Shortest Path First)* es un algoritmo caracterizado por que el envío del paquete siempre se realiza por la ruta más corta de todas las disponibles, que siempre es la que requiere un número menor de saltos. Es muy común en las LAN y se utiliza en routers interiores y de borde. Inicialmente se introdujo como una mejora de RIP, por lo que puede convivir con él. Supera la limitación de los 15 saltos como máximo de RIP.
- **IS-IS** *(Intermediate System to Intermediate System)* es un algoritmo propuesto por la ISO para comunicar sistemas intermedios *(intermediate systems),* que es el nombre que emplea la ISO para denominar a los enrutadores. Solo se utiliza en router interiores. Se usa menos que OSPF.

Ampliación

Los protocolos de enrutamiento híbridos son protocolos de encaminamiento que utilizan técnicas tanto de vector-distancia como de estado de enlace para calcular sus tablas de rutas. El protocolo de enrutamiento híbrido más utilizado es EIGRP *(Enhanced Interior Gateway Routing Protocol).*

Algunas características de **EIGRP** son las siguientes:

- Se utiliza en routers interiores y de borde.
- Es un protocolo propietario de Cisco, por lo que solo es compatible con enrutadores de este fabricante. En redes en los que todos los enrutadores son de Cisco es mejor utilizar EIGRP, pero en aquellos en los que haya enrutadores de otros fabricantes hay que utilizar OSPF.
- Su tiempo de convergencia es mínimo.
- Genera muy poco tráfico específico de enrutamiento, por lo que consigue un mejor rendimiento en la transmisión de paquetes de datos de usuario.

Parámetro	RIPv1	RIPv2	IGRP	OSPF	EIGRP
Tipo	Vector-distancia	Vector-distancia	Vector-distancia	Estado enlace	Híbrido
Coste	120	120	100	110	90 (ruta interna) o 170 (ruta externa)
Tipo de red enrutada	De clase	Subnetting	De clase	Subnetting	Subnetting
Métrica	Número de saltos	Número de saltos	Ancho de banda y latencia	Coste y ancho de banda	Ancho de banda y latencia
Mensajes a otros enrutadores	Broadcast (255.255.255.255)	Multicast (224.0.0.0)	Broadcast (255.255.255.255)	Multicast (224.0.0.5 y 224.0.0.6)	Multicast (224.0.0.10)
Tiempo convergencia	Lento	Lento	Lento	Rápido	Rápido
Escalabilidad	Pobre	Baja	Alta	Alta	Alta

Tabla 6.1. *Comparativa de las características básicas de distintos protocolos de enrutamiento.*

2.2. Configuración del enrutamiento

Cada nodo de una red IP debe tener configurados sus parámetros de red. Desde el punto de vista del enrutamiento, el parámetro más significativo es la puerta por defecto.

A. Rutas de protocolo IP

Cuando el emisor y el receptor de un paquete IP están en la misma red lógica no hay problemas de comunicación porque el emisor sabe que el receptor está en su misma red mediante ARP y, por tanto, todo lo que él escriba en la red será leído por el receptor. Sin embargo, cuando emisor y receptor están en distintas subredes, es muy posible que el emisor no sepa qué tiene que hacer para que el paquete llegue a su destino.

Una **ruta** es la dirección IP de un nodo (router) que tiene suficiente inteligencia electrónica (algoritmos de encaminamiento) para saber qué hacer con un paquete IP que ha recibido de un nodo de la red con objeto de que llegue a su destino, o al menos saber a quién puede enviárselo para que lo resuelva en su nombre, es decir, que una ruta es un apuntador IP a un encaminador. El router decide qué línea de transmisión utilizar para alcanzar su objetivo.

Cuando se utilizan los servicios de una ruta por defecto y la dirección del paquete no puede ser resuelta, se devolverá un mensaje al nodo emisor indicándole que el nodo o la red a la que se destina el paquete IP es inalcanzable.

Las rutas de cualquier nodo, y especialmente las de un encaminador, están recogidas en una o varias tablas de encaminamiento que son utilizadas por el servicio de enrutamiento de red para determinar los caminos que deben seguir los paquetes IP para alcanzar su destino. Las rutas pueden tener atributos; por ejemplo, pueden ser dinámicas, si se crean automáticamente en cuanto varía la estructura de la red mediante apertura de conexiones, y estáticas o persistentes, si se crean en tiempo de arranque del sistema del enrutador.

Vocabulario

Ruta de encaminamiento o simplemente **ruta:** es la dirección IP de un nodo (router) que tiene suficiente inteligencia electrónica (algoritmos de encaminamiento) para saber qué hacer con un paquete IP con objeto de que llegue a su destino, o al menos a quién puede enviárselo para que lo resuelva por él.

Ruta por defecto o ***default gateway:*** es la ruta a la que se envía un paquete cuando ninguna otra ruta es apropiada para ello, con la confianza de que el router al que apunta sepa cómo distribuir el paquete. En el mundo TCP/IP, especialmente sobre Linux, nos encontraremos que a la ruta por defecto se la denomina *gateway*, aunque el término *gateway* (pasarela) formalmente significa, según la terminología OSI, una máquina de nivel superior al nivel 4.

Ampliación

Modo de nombrar la red IP a la que pertenece un nodo

El modo en que se nombran las redes IP es semejante al que se utiliza para los nodos. Si tenemos una red 10.130.5.10 con máscara 255.255.0.0, la red a la que pertenece ese nodo se nombrará como red 10.130.0.0, aunque algunos sistemas utilizan la nomenclatura 10.130 en la que los ceros se suprimen. La ruta por defecto se representa por la secuencia 0.0.0.0.

Como se ve, la red a la que pertenece un nodo se nombra por la parte de la dirección IP del nodo que se corresponde con la secuencia de «1» en su máscara de red.

Otros ejemplos serían los siguientes:

- 10 es la red del nodo 10.3.23.67/8.
- 192.168 es la red del nodo 192.168.2.55/16.
- 192.168.2 es la red del nodo 192.168.2.55/24.

Cuando las máscaras son distintas de las redes de clase (8, 16 o 24 bits), nombrar la red es algo más complejo, como ya se estudió durante el desarrollo de la tecnología de subnetting.

Truco

En Windows la orden utilizada para gestionar la tabla de rutas es ROUTE. En Linux suele utilizarse la orden **iptables** e **ip route.** Se puede conseguir información sobre estas órdenes en el calificador de ayuda de la orden. La ejecución de estas órdenes con los calificadores que implican una modificación de la configuración de rutas implica la posesión de permisos de administrador del sistema.

B. Configuración de la tabla de rutas

En la Fig. 6.5 hay un ejemplo de una tabla de rutas sobre un cliente Windows con un acceso a la red de área local, que vamos a analizar detenidamente para hacernos una idea de la información que contiene y cómo se utiliza.

No todas las tablas de rutas son iguales, dependen del sistema operativo en el que operan; sin embargo, la mayoría de las tablas de rutas tienen los siguientes atributos:

- **Destino de red.** Es el nombre de la red que se pretende alcanzar.
- **Máscara de red.** Define la máscara de red de destino. La máscara de red junto con el destino de red definen el conjunto de nodos de red a los que se dirige la ruta.
- **Puerta de acceso o puerta de enlace.** Es la dirección IP del router (*gateway* o puerta de acceso en la terminología de la arquitectura IP), que debe ser capaz de resolver los paquetes que se dirijan a ese destino de red. Cuando la puerta de enlace coincide con la propia red local es señal de que el destino se alcanza inmediatamente por alguna de las interfaces de red local.
- **Interfaz.** Es la dirección IP o, en ciertos casos, el nombre de la interfaz de red que la posee por el que se deben enviar los paquetes de datos para alcanzar la puerta de enlace.
- **Métrica.** Es un parámetro que define una medida del coste telemático que supone enviar el paquete a la red destinataria a través de la puerta de acceso.

En Windows la orden apropiada para gestionar la tabla de rutas es **ROUTE ADD** para añadir rutas y **ROUTE DELETE** para borrarlas. Se puede acompañar de un calificador (–P) que hace que la ruta añadida sea permanente, es decir, que cuando se inicie de nuevo el sistema operativo la ruta seguirá estando definida a no ser que antes le hayamos aplicado una orden ROUTE DELETE que la elimine.

Además habrá que especificar la dirección de la red de destino junto con su máscara y la puerta de enlace, es decir, la dirección del enrutador que aceptará peticiones hacia esa red. Por ejemplo, si el nodo local tiene una dirección 192.168.1.1/24 y ejecutamos la siguiente orden:

ROUTE ADD –P 192.168.201.0 MASK 255.255.255.0 192.168.1.254

Entonces el sistema entenderá que cuando se quieran enviar paquetes a la red 192.168.201.0/24 (obsérvese que los nodos de esta red no pueden verse directamente desde el nodo local que es 192.168.1.1) deberá enviarlos al enrutador 192.168.1.254 (que sí es alcanzable por el nodo local), para que este gestione el envío hacia su destino. Además, como hemos proporcionado el calificador –P, la ruta será persistente.

Si la especificación de la red de destino hubiera sido 0.0.0.0, entonces la ruta declarada se correspondería con la ruta por defecto.

Ejemplos

En la declaración de la orden ROUTE se pueden utilizar nombres simbólicos en vez de usar las direcciones numéricas de hosts y redes. En este caso, los nombres simbólicos de redes deben estar declarados en el fichero de Windows C:\WINDOWS\SYSTEM32\DRIVERS\ETC\NETWORKS. De modo semejante, los nombres simbólicos de hosts deben estar declarados en el fichero de Windows C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS.

Otro calificador que puede ser útil en la orden ROUTE es –f. Este calificador borra la tabla de enrutamiento en curso para iniciar una nueva configuración limpia de las rutas del sistema. Si el calificador –f se usa dentro de un comando cualquiera, se ejecutará el comando después del borrado de las rutas en la tabla de rutas.

Por último, la orden **ROUTE CHANGE** se utiliza para hacer cambios en rutas existentes, por ejemplo, si sobre la orden anterior se quiere hacer el cambio de puerta para que tome el nuevo valor 192.168.1.250, ejecutaríamos la orden:

ROUTE CHANGE 192.168.201.0 MASK 255.255.255.0 192.168.1.250

en donde ya no sería necesario el calificador de persistencia –P, ya que este solo se toma en cuenta junto con el comando ADD.

Ejemplos

Reconocer los elementos de una tabla de rutas en un nodo Windows

Fijémonos en la Fig. 6.5, que visualiza la ejecución de la orden **route print** sobre un sistema Windows XP. En primer lugar observamos que hay dos interfaces reales: la de la red de área local inalámbrica (de Intel) y otra denominada *Loopback*. Esta última es el modo en que TCP/IP comunica aplicaciones dentro del mismo nodo, utilizando la dirección de la red 127.0.0.0, que queda reservada para este propósito. De hecho, 127.0.0.1 es el propio nodo local o «local host».

En segundo lugar, observamos la ruta 192.168.1.0 con máscara 255.255.0.0. Define una puerta de acceso que es 192.168.1.137, que es el mismo nodo local. En efecto, cuando el nodo quiere enviar un paquete a otro nodo de su misma red no necesita mandarlo a ningún router y directamente lo pone en su tarjeta de red (192.168.1.137).

La puerta de enlace predeterminada es 192.168.1.1, que sería la dirección del router que resolvería cualquier destino que ninguna otra ruta pueda resolver.

La última línea, que tiene como destino de red 255.255.255.255, es muy especial. Se refiere a los paquetes *broadcast* de la red y, por tanto, tiene un funcionamiento diferente. Al final aparecería una colección de rutas persistentes o estáticas, que en el ejemplo de la figura está vacía.

Cuando un paquete IP alcanza a un nodo, sea o no un router, se compara la dirección de destino con las entradas de la tabla de rutas para averiguar si ese nodo es el destinatario o, en caso contrario, si debe reexpedirlo por alguna de sus interfaces de red. Es posible que un destino se alcance por varias rutas; en ese caso, el software de enrutamiento elige la mejor ruta basándose en las especificaciones de las métricas de cada ruta. Si el destino no se alcanzara por ninguna entrada, entonces se utilizará la ruta por defecto si existe. Si no estuviera definida, se generará un mensaje de error, puesto que el destino sería inalcanzable.

Hay que hacer unas últimas observaciones. La dirección de un nodo y la de su pasarela por defecto deben estar en la misma red; de lo contrario, no podrán verse y el encaminamiento no funcionará. En segundo lugar, hay que tener en cuenta que por cada interfaz de red se puede definir más de una ruta. Y por último, si la tabla de rutas es grande, se ralentizará excesivamente el proceso de análisis: no hay que olvidar que esta comparación con la tabla de rutas debe hacerse con cada paquete IP que llegue al router.

Veamos la ejecución de una orden **route print** en Windows 7 (Fig. 6.6). En primer lugar se observa que hay una interfaz de red real (Adaptador de red Broadcom 802.11n). El resto de las tarjetas de red que aparecen son virtuales y tienen funciones especiales. A la izquierda de estas tarjetas de red se pueden ver las direcciones físicas asociadas a cada interfaz (C4:46:19:1B:45:B1 para la interfaz física considerada anteriormente).

También se puede ver un adaptador especial denominado *Software Loopback Interface,* que es el utilizado por el sistema operativo para comunicar aplicaciones dentro del mismo nodo utilizando TCP/IP. Se corresponde con la dirección de red 127.0.0.0. De hecho, el propio nodo se direcciona localmente como 127.0.0.1, que es una dirección reservada y que se puede nombrar como «local host». Su dirección equivalente en IPv6 es «::1».

El mapa de rutas es semejante al visto para Windows XP, pero al final del mismo aparece una extensión para el sistema de enrutamiento para IPv6, que viene instalado por defecto en Windows 7 y no en Windows XP.

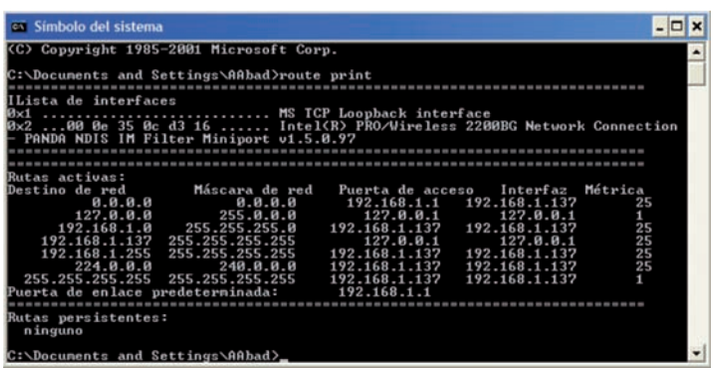


Fig. 6.5. *Tabla de rutas en un nodo Windows XP.*

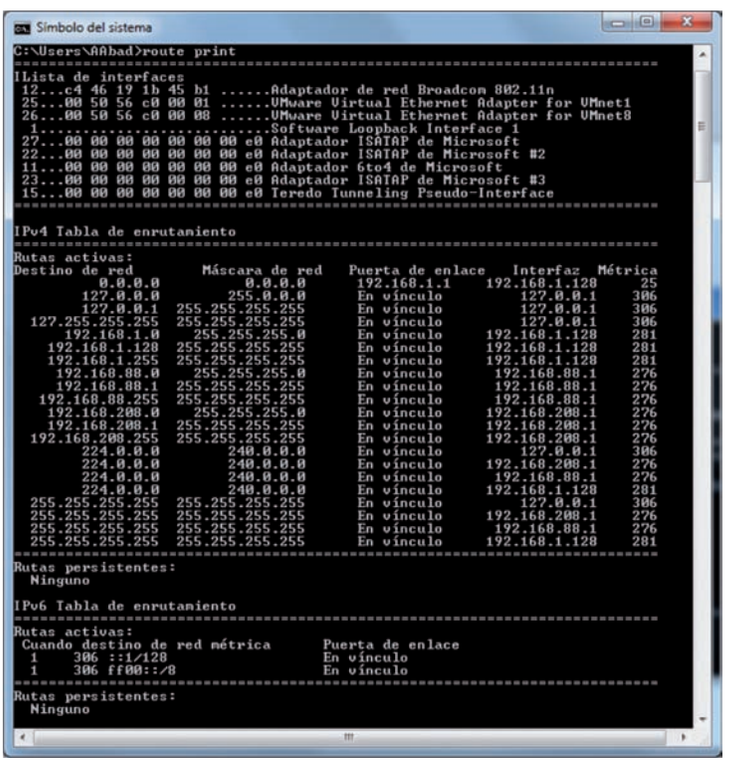


Fig. 6.6. *Tabla de rutas en un nodo Windows 7.*

Ejemplos

Reconocer los elementos de una tabla de rutas en un nodo Linux

En la Fig. 6.7 podemos observar el resultado de la orden **ip route show** sobre un sistema Linux, que sirve para pedir información relacionada con las rutas del nodo sobre el que se ejecuta.

El resultado en este caso es de tres líneas, de las que nosotros nos fijaremos en la primera y en la tercera. En la primera línea se especifica el nombre de la red IP, que es 192.168.1.0/24, la interfaz de red asociada (eth1) y la dirección IP en esta interfaz que corresponde al nodo local (192.168.1.34), que obviamente deberá estar en el ámbito de la red (192.168.1.0/24).

En la tercera línea se especifica la ruta por defecto *(default)*. Esta línea se interpreta como que el *default gateway* del sistema se puede conseguir por la interfaz eth1 (dev eth1), siendo la dirección IP del enrutador *(default Gateway)* 192.168.1.1.

Obsérvese que la dirección del enrutador de la red local está en la misma red local que la dirección IP local, de lo contrario el nodo local no podría comunicar con su enrutador más próximo y el nodo quedaría aislado.

```
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
aabad@ptx:~$ ip route show
192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.34
169.254.0.0/16 dev eth1  scope link  metric 1000
default via 192.168.1.1 dev eth1
aabad@ptx:~$
```

Fig. 6.7. *Tabla de rutas en un nodo Linux.*

En Linux, el sistema de creación de nuevas rutas es semejante al visto anteriormente para Windows. En este caso se utiliza la orden **ip route add,** que también admite muchos calificadores. Como siempre, la recomendación habitual cuando se usa Linux es consultar la ayuda del distribuidor de software o la ayuda de la orden para conocer con precisión los parámetros que admite y su forma de uso.

Si el nodo local tuviera, como antes, la dirección 192.168.1.1/24, y ejecutamos en Linux la orden:

ip route add –net 192.168.201.0/24 gw 192.168.1.254 dev eth0

Entonces tendríamos declarada la misma ruta que hemos creado antes sobre Windows. En este caso hemos declarado que la interfaz por donde se alcanza el router es eth0 (en Windows también se podría especificar, aunque, si se omite, Windows selecciona automáticamente la interfaz compatible con la dirección del encaminador).

2.3. Interconexión de encaminadores

Un encaminador resuelve las rutas de los paquetes cuyo destino se encuentra en alguna de las interfaces de red que posee o bien delega esta función en otro encaminador próximo.

Es evidente que el enrutador corporativo no puede tener una interfaz de red por cada posible red de destino, por lo que no sería capaz de resolver el destino de la mayor parte de los paquetes.

Para solucionar esto, los enrutadores se configuran estableciendo relaciones de unos con otros. El nexo lógico de unión entre dos encaminadores son las entradas de la tabla de rutas en que se hacen referencia entre sí. De este modo, cuando un router recibe un paquete, consulta su tabla de rutas para averiguar si es capaz de resolver el destino. Si no encuentra la dirección en su tabla de rutas, entonces encamina el paquete hacia un encaminador de orden superior confiando en que él sepa resolverlo.

Ejemplos

Configuración de red con dos encaminadores

Vamos a estudiar un ejemplo de configuración en el que dos nodos se sitúan en segmentos de red distintos e interconectados a través de un encaminador. Este encaminador se conecta a un segundo enrutador para su salida al exterior de la red (Fig. 6.8).

En el diagrama de red se pueden ver tres redes distintas configuradas con dos nodos, uno en la red1 y otro en la red2, y dos routers, uno llamado Router1, que conecta las redes de los dos nodos, y otro Router2, que se utilizará como *gateway* por defecto. En la parte inferior aparece una tabla simplificada de las rutas más específicas que tendrán que crearse en el Router1. El gráfico nos va a servir para explicar los dos casos siguientes.

Comunicación de dos nodos con rutas conocidas

Supongamos que el nodo1 de la red1 quiere enviar un paquete IP al nodo2 situado en la red2. Puesto que el nodo2 no está en la misma red lógica que el nodo1, este le enviará el paquete IP al Router1, al que descubrirá por estar escrito en su tabla de rutas como pasarela por defecto, para que cumpla con su función de encaminamiento.

Una vez que el paquete llega al Router1, este comparará la dirección de destino (209.85.15.20) con las entradas de su tabla de encaminamientos y observará que hay una ruta (la número 1) que alcanza la red2, y ello lo consigue si reexpide el paquete a través de su interfaz de red NICr2. Una vez escrito el paquete IP en la red2, ya habrá acabado su función logrando su objetivo porque no hay que dar un salto posterior (la red se alcanza como vínculo local).

Comunicación a través de la ruta por defecto

Imaginemos ahora el caso de que el nodo1 quiere enviar un paquete IP a una dirección cualquiera que no se encuentra ni en la red1 ni en la red2. En ese caso, cuando el paquete llegue al Router1, configurado como ruta por defecto del nodo1, se examinará la tabla de rutas para ver si existe alguna entrada capaz de alcanzar el destino. Como el Router1 no tiene ninguna entrada con ese destino, utilizará la ruta por defecto, que en este caso apunta al router externo cuya dirección es 65.23.4.1, que será previsiblemente capaz de resolver el destino. Para alcanzar su objetivo, el Router1 sabe que con ese salto no se alcanza el destino ya que su siguiente salto es el Router2.

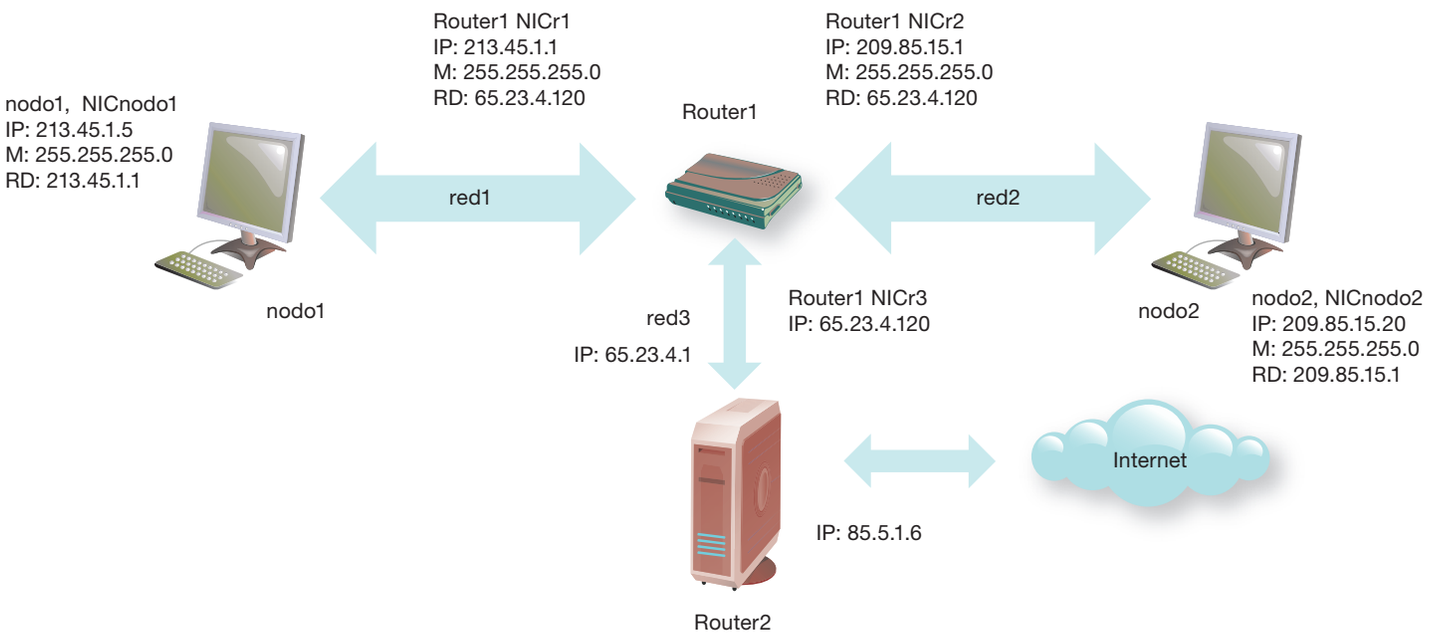


Fig. 6.8. *Ejemplo gráfico de enrutamiento IP.*

Número ruta	Red destino	Máscara	Puerta acceso	Interfaz	Siguiente salto
1	209.85.15.0	255.255.255.0	209.85.15.1	NICr2	Vínculo local
2	213.45.1.0	255.255.255.0	213.45.1.1	NICr1	Vínculo local
3	0.0.0.0	255.255.255.255	65.23.4.1	NICr3	Router2

Investigación

En la página web **http://www.wikilearning.com/tutorial/manual_practico_de_iptables-que_es_un_firewall/9755-1** puedes encontrar un completo manual de **iptables** junto con una descripción de lo que es un cortafuegos. Tiene mucho interés que te familiarices con la estructura de calificadores de esta orden porque es ampliamente utilizada en el mundo Linux. Te puede ser de gran utilidad confeccionarte una tabla con los calificadores más importantes. Puedes ayudarte también de la información que hay en la página web **https://www.ac.usc.es/docencia/ASRII/Tema_4html/node6.html**

Ampliación

Entre las ventajas que aporta la tecnología NAT se encuentran:

- Ahorro de direcciones IPv4 públicas, que están prácticamente agotadas.
- Mejoras en la seguridad de la LAN al hacer ocultas las direcciones IP privadas al exterior.
- Permite a los administradores de red desarrollar su propio sistema de direccionamiento IP interno.

Cuando NAT sustituye una dirección privada con otra pública elegida arbitrariamente entre todas las IP públicas contratadas disponibles, se habla de **DNAT** *(Dynamic Network Address Translation)* o formalmente *IP Masquerading*. En cambio, cuando la asignación de la IP pública se define específicamente sin dejar capacidad de elección al sistema, entonces se habla de **SNAT** *(Static Network Address Translation)*.

Cuando se desarrolle la teoría sobre cortafuegos se ampliará la información sobre los protocolos de traducción, entre otros **PAT** *(Port Address Translation)* para la traducción de puertos.

2.4. Enmascaramiento IP

El enmascaramiento IP *(IP Masquerading)* es una función de red de algunos sistemas operativos actuales que permiten la conexión de otros miembros de la red a Internet a través de la conexión que ya posee la máquina que soporta el enmascaramiento. Para el correcto funcionamiento del *IP Masquerading* no es necesario que todas las estaciones de la red tengan una dirección IP única y pública de Internet; basta con que tengan la pila de protocolos IP y correctamente configurado su sistema de rutas. Analicemos con un ejemplo cómo funciona esta técnica. La función de *IP Masquerading* también la realiza el protocolo **NAT** *(Network Address Translation)*.

Supongamos que tenemos un host, que llamaremos CLIENTE y que tiene por dirección IP 10.1.1.5 y máscara de toda la red 255.0.0.0, que quiere acceder a Internet solicitando páginas a través de su navegador. La conexión a Internet se ha realizado en otro host de la red al que llamaremos SERVIDOR con dirección IP 10.1.1.1 y que está en la misma subred que CLIENTE.

Cuando SERVIDOR realiza una conexión a Internet, su proveedor le proporciona una dirección IP a la interfaz de red WAN por la que se conecta remotamente que es 213.97.2.12.

Debemos tener en cuenta que los pasos 1 y 4 se producen dentro de una LAN, mientras que los números 2 y 3 proceden de una WAN.

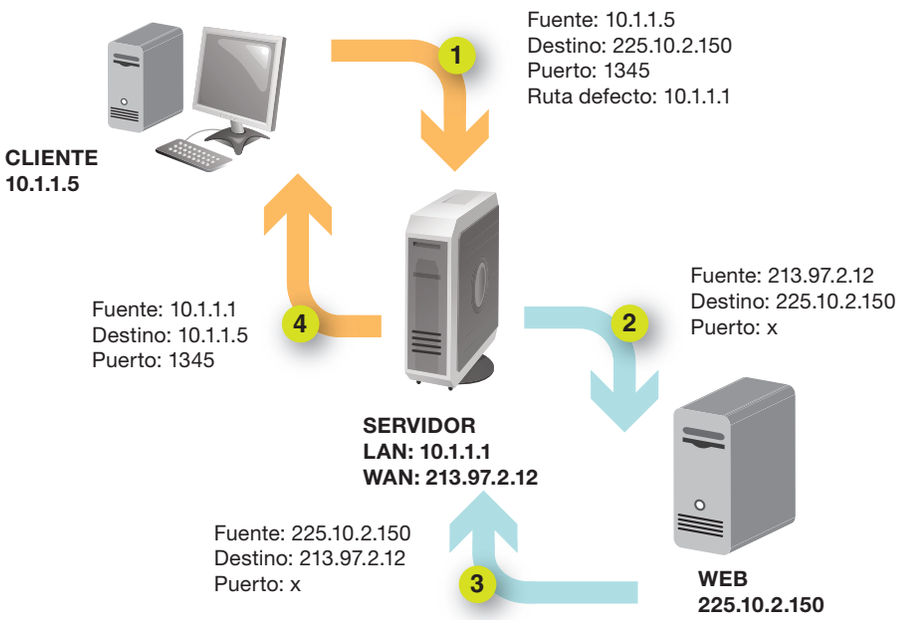


Fig. 6.9. *Esquema de un ejemplo de utilización de enmascaramiento IP.*

En CLIENTE, configuramos TCP/IP para que la ruta por defecto apunte a SERVIDOR. Por otra parte, por ejemplo, el navegador pediría datos utilizando un puerto que el servidor que le brinde las páginas aprovechará para enviárselas con la seguridad de que el navegador se quedó escuchando por ese puerto.

Si el navegador en CLIENTE solicita una página al servidor 225.10.2.150 por el puerto 1345, como CLIENTE no tiene acceso por red al host 225.10.2.150, mandará el mensaje por la ruta de defecto a SERVIDOR. Si SERVIDOR tiene habilitado el servicio de enmascaramiento, sustituirá la dirección IP de CLIENTE por la suya propia en la interfaz WAN (213.97.2.12) y el número de puerto por otro que tenga libre, haciéndole la petición al servidor web de dirección 225.10.2.150. Cuando el servidor web le conteste, SERVIDOR sustituirá la dirección IP WAN suya (213.97.2.12) por la dirección IP propia en su red de área local (10.1.1.1) y se lo mandará a CLIENTE por el puerto por el que este se quedó esperando, en nuestro ejemplo, el 1345. De este modo, CLIENTE ha recibido sus datos transparentemente.

3. El cortafuegos

Abrir la propia red de área local al mundo exterior de Internet, que es absolutamente público y mayoritariamente incontrolado, puede ser peligroso para la organización, ya que pueden producirse accesos indebidos desde el exterior, desde los de simples curiosos hasta los procedentes del espionaje de la competencia.

3.1. Características generales

Es conveniente que las organizaciones restrinjan los accesos a su red desde el exterior. Para ello se instala en el perímetro de la red un nodo especial denominado cortafuegos o *firewall* que se encarga de limitar los accesos en ambas direcciones, haciendo invisible la red de área local desde el exterior o restringiendo los accesos desde dentro hacia afuera.

En general, un cortafuegos tiene que proporcionar tanto seguridad en los accesos como transparencia en los envíos de datos.

Actividades

3. Confirma la veracidad de las siguientes afirmaciones:

a) El encaminador opera siempre en el nivel 3 de OSI.

b) Algunos encaminadores toman funciones de niveles superiores al 3.

c) Un router solo puede encaminar paquetes IP.

d) Todos los protocolos de red son encaminables con el router adecuado.

e) Los routers no pueden encadenarse en cascada.

4. Escribe en la columna de la derecha el nombre de la red del nodo que aparece en la de la izquierda. La primera línea te servirá como ejemplo:

Nodo	Red
10.0.1.88/24	10.0.1
192.168.1.1/16	
192.168.1.1/8	
192.168.1.1./32	

5. Preséntate en una máquina Windows como administrador del sistema para que puedas modificar los parámetros de red.

a) Crea una ruta para alcanzar la red 192.168.30 por el enrutador 192.168.30.254.

b) Crea una ruta que alcance la red 192.168 por el enrutador 192.168.101.254.

c) Visualiza las rutas para comprobar que están creadas correctamente.

d) Borra las dos rutas.

6. Repite el ejercicio anterior sobre una estación Linux.

7. Confirma la veracidad de las siguientes afirmaciones:

a) Los encaminadores pueden ser abiertos, cerrados o de frontera.

b) Los algoritmos de encaminamiento estático son aquellos que impiden que se cambien las tablas de rutas del encaminador en el que se ejecutan.

c) Un algoritmo de encaminamiento adaptativo habilita al router para aprender por sí mismo la topología de la red.

d) El coste de una ruta es el precio económico que se ha de pagar por transmitir un paquete.

e) El tiempo de convergencia es el tiempo que tarda un router en arrancar desde que se enciende hasta que queda operativo.

8. Relaciona los elementos de la columna de la izquierda con los de la derecha:

Tipo de protocolo de enrutamiento	Protocolo de enrutamiento
IGP	RIPv1 o RIPv2
EGP	BGP
	OSPF
	IS-IS
	EIGRP

CEO

SMR_RL_AAbad_06_Cortafuegos.docx

Documento que contiene información sobre cortafuegos personales y corporativos.

Hay cortafuegos que operan en muy distintos niveles de la arquitectura OSI. Así, un cortafuegos que opere en niveles bajos será más fácilmente configurable pero menos flexible. Por ejemplo, una vez que se ha establecido la conexión lícitamente, la misión del cortafuegos se extingue. Otros *firewalls,* sin embargo, operan en los niveles superiores e investigan en el interior de cada paquete de datos, lo que los hace lentos pero extraordinariamente flexibles.

Los cortafuegos suelen configurarse mediante políticas o reglas que se establecen en función del origen, del destino y del protocolo utilizado. Por defecto, un cortafuegos cierra toda comunicación. Es el administrador de red quien tiene que abrir los diferentes puertos de comunicación y habilitar los flujos de transporte permitidos.

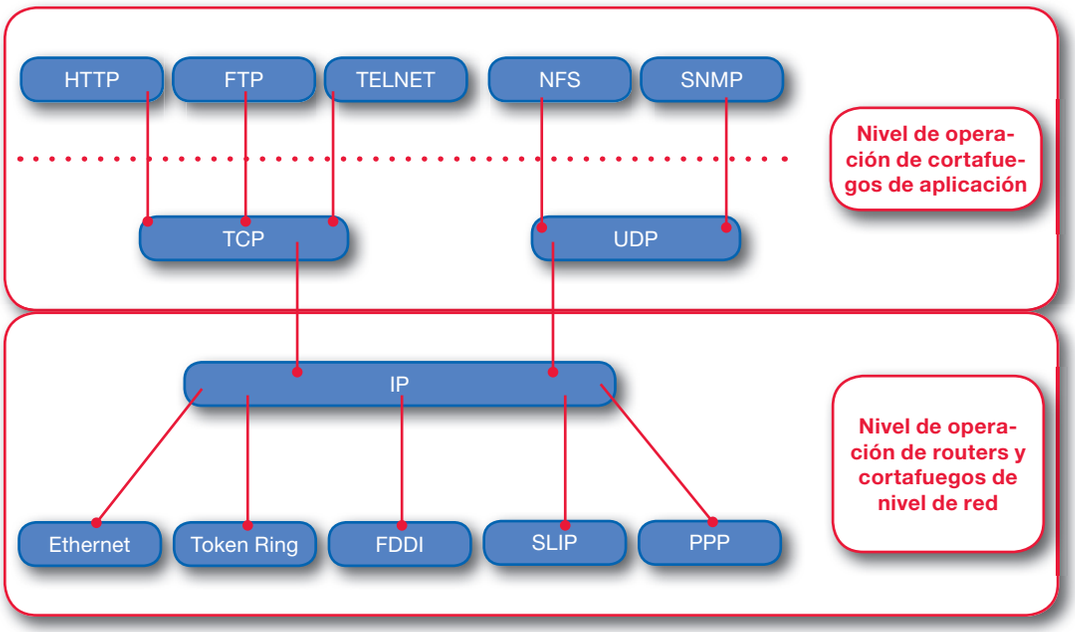


Fig. 6.10. *Niveles de operación de los cortafuegos de nivel de red y de aplicación.*

Además, si el cortafuegos opera en un nivel elevado, puede incluir nuevas funcionalidades, por ejemplo, en la admisión de correo electrónico a través del puerto 25 puede analizarse el contenido para explorar si el mensaje incorpora algún virus.

Cuando un equipo conectado a la red pierde su conexión, lo primero que hay que hacer es comprobar el sistema de cableado pero, inmediatamente después, debemos sospechar del cortafuegos del equipo, que puede estar impidiendo las conexiones desde o hacia el exterior del equipo por un error en la configuración de las políticas de acceso a la red.

Ampliación

En la actualidad los cortafuegos operan en las capas superiores y pueden incorporar nuevos valores añadidos que mejoran la seguridad (Fig. 6.10). Algunos de estos valores se citan a continuación:

Traducción de direcciones NAT. Consiste en que las direcciones IP utilizadas por los hosts de la Intranet solo tienen validez dentro de la propia red de área local. El cortafuegos se encarga de sustituir cada dirección IP de la Intranet en los paquetes que entran y salen a su través por otras direcciones IP virtuales, protegiendo de este modo contra accesos indeseados a través de direcciones Internet que realmente no existen en la Intranet. NAT es un caso particular de *IP Masquerading*.

Traducción de direcciones y puertos NAPT *(Network Address Port Translation).* Es una variación de NAT en donde no solo se sustituyen las direcciones IP sino también los números de puertos. En ocasiones a este protocolo también se le llama **PAT** *(Port Address Translation),* que es una nomenclatura propia de Cisco. Se trata de sustituir el puerto de escucha del segmento de salida por otro que queda abierto en la interfaz de salida del *gateway* (o cortafuegos) y que enmascara al original. PAT ofrece una mejora de la seguridad de las aplicaciones locales ocultando su puerto de escucha y además asigna automáticamente puertos a las aplicaciones que se lo solicitan.

Protección frente a virus. Al operar en las capas altas, estos cortafuegos son capaces de analizar la información que fluye hacia la Intranet, y pueden detectar anomalías en los datos y programas.

Auditoría. El cortafuegos puede auditar recursos concretos de la Intranet y avisar a través de un sistema de mensajería electrónica del intento de violación de algún recurso o de accesos indebidos.

Gestión de actividad. A través de agentes SNMP o DMI, propios de gestión de red, se puede monitorizar el cortafuegos con el fin de realizar informes sobre la actividad de la red.

3.2. Zonas desmilitarizadas

Una red desmilitarizada o **DMZ** *(Demilitarized Zone)* es una red compuesta por uno o más ordenadores que, en la instalación de red, se sitúan lógicamente entre la red corporativa, que se supone segura, e Internet, que es insegura. Los servicios típicos que se ubican en una DMZ son servidores web, ftp, de correo y DNS.

Existen muchas posibilidades para la construcción de una DMZ. Aquí nos fijaremos en algunas de ellas, pero todas tienen que cumplir su principal misión, que consiste en que se proporcionen servicios públicos a Internet sin comprometer la seguridad de los datos alojados en la red corporativa.

En el primer modelo de DMZ expuesto (Fig. 6.11-A), tanto la red corporativa como la DMZ se conectan a Internet a través de un router. La protección de la DMZ reside en la protección de cada uno de los servidores más el filtrado que pueda realizar el encaminador.

Sin embargo, la red corporativa queda protegida por un cortafuegos. Ninguna conexión procedente de Internet debe alcanzar a la red corporativa, pues toda la información disponible para Internet debe residir en la DMZ.

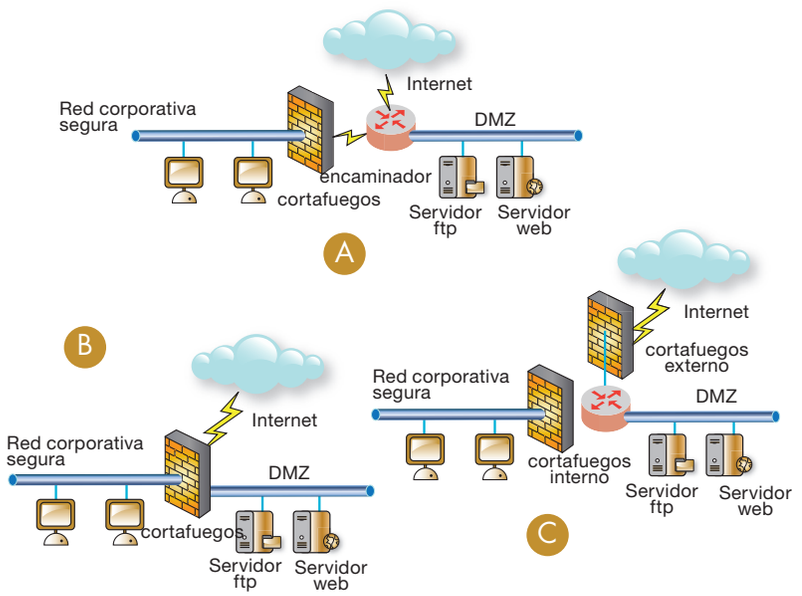


Fig. 6.11. *Tres modelos para una DMZ.*

En el segundo modelo (véase Fig. 6.11-B), tanto la red corporativa como la DMZ quedan protegidas por el cortafuegos. Esta configuración, que es la más común, requiere que el cortafuegos tenga definida una tercera red para la construcción de la DMZ. El filtrado de las conexiones será mucho más restrictivo en la red corporativa que en la DMZ.

En el tercer modelo que estudiaremos, la arquitectura de la red se complica (Fig. 6.11-C). En este caso, la DMZ queda encerrada entre dos cortafuegos. Obviamente es la configuración más segura, pero también la más costosa.

La configuración de la DMZ dependerá de la arquitectura de ella y de su relación con la red interna (protegida) y la externa. Según esto, el cortafuegos que hace de frontera entre la DMZ, la LAN e Internet debe establecer tres tipos de políticas de comunicación diferenciadas entre ellas:

a) **Políticas de relación LAN con Internet.** Estas directivas configuran el acceso de los usuarios de la LAN a Internet, por ejemplo, con servicios como navegación.

b) **Políticas de relación LAN con la DMZ.** Aquí se configurará cómo los usuarios de la LAN pueden acceder a los servicios provistos por los servidores ubicados en la DMZ, por ejemplo, para actualizar la información de las páginas web de un servidor web que se ubique en la DMZ.

También aquí debe configurarse cómo los servidores de la DMZ pueden acceder a los servicios ofrecidos desde la LAN. Cuanto menos restrictivos se sea aquí, menor grado de protección se tendrá.

Vocabulario

En la documentación técnica es frecuente referirse a las zonas desmilitarizadas como redes perimetrales o, de modo más simple, referirse al perímetro. Así, para expresar que un servidor está situado en una **DMZ** podremos decir que es un servidor del perímetro.

Investigación

En **http://bookalexa.blogspot.com/2008/02/perimetro-de-seguridad.html** tienes información sobre qué elementos en una red perimetral pueden ayudar a fortalecer la seguridad de una DMZ. Léela atentamente para hacerte una idea de los riesgos a que están expuestos los hosts que tienen un contacto perimetral con Internet y la forma en que se previenen.

Para instalaciones en entornos colaborativos, también puedes consultar la dirección **http://www.microsoft.com/spain/exchange/securemessaging/seguridad.mspx**

c) **Políticas de relación DMZ con Internet.** Aquí se configura cómo los usuarios de Internet (supuestamente anónimos) acceden a los servicios publicados por los servidores de la DMZ.

Para clarificar cómo puede cooperar una DMZ con la seguridad de la instalación de red, tomemos como ejemplo la instalación de una sede de comercio electrónico.

El comprador accede a la página web del vendedor a través de Internet y selecciona el artículo que desea comprar. Al servidor web, que estará situado en la DMZ del vendedor, se accede con una dirección IP pública, que puede ser propia del servidor web o la del encaminador o cortafuegos externo del vendedor, dependiendo de la configuración DMZ elegida. En cualquiera de los casos, la petición http del comprador debe llegar al servidor web situado en la DMZ.

La página web recoge información del cliente y la escribe en una base de datos. Es muy peligroso que esta base de datos resida en Internet o en una DMZ, puesto que los equipos situados en estas zonas de la red están expuestos a ataques. El diseñador de la aplicación ha resuelto que la base de datos debe residir en un servidor dentro de la red corporativa mucho más segura.

Por tanto, el administrador de la red tiene que definir unas políticas de acceso de modo que:

- Ninguna conexión procedente de Internet pueda acceder al servidor de bases de datos de la red corporativa.
- A esa base de datos solo puede acceder el servidor web situado en la DMZ y además exclusivamente a los puertos específicos para el acceso a la base de datos y no a otros.

De este modo, si un intruso quiere acceder a la red corporativa, el cortafuegos se lo impedirá; solo puede acceder al servidor web de la DMZ.

Si este servidor tuviera un agujero de seguridad y se hiciera con su control, solo podría acceder al servidor de bases de datos de un modo restringido.

Actividades

9. Comprueba si son ciertas o falsas las siguientes afirmaciones:

a) Un cortafuegos siempre impide el paso de paquetes de red.

b) El *firewall* siempre impide el paso a los paquetes entrantes, pero permite el paso de paquetes de red salientes.

c) El cortafuegos opera siempre en los niveles más altos de OSI.

d) El protocolo PAT de Cisco equivale exactamente al protocolo NAT.

e) El cortafuegos por antonomasia en Linux es iptables.

10. Busca los errores técnicos en el siguiente comentario:

«Para proteger una red de área local de los accesos indebidos desde la red externa se ha instalado un cortafuegos al que se conectan la red local, Internet y una red perimetral. Para que un paquete de red procedente de Internet llegue a la red desmilitarizada, previamente debe pasar por la red local protegida. Sin embargo, los paquetes con destino en Internet que proceden de la red local no es necesario que pasen por el cortafuegos ya que los riesgos siempre están en la red externa.»

11. Para realizar este ejercicio necesitas tener acceso a un router con capacidades de cortafuegos y gestión de una DMZ. Muchos de los enrutadores que suministran los proveedores de Internet de banda ancha tienen esta capacidad y te pueden servir.

a) Accede a la página web de gestión del router por su dirección IP y comprueba que tienes activada la función de cortafuegos o que tienes habilitado el protocolo NAT.

b) Ahora crea una zona DMZ (en estos encaminadores sencillos, la DMZ suele corresponderse con una red de un único nodo en donde se supone que se instalará el bastión de la DMZ que publicará servicios hacia Internet).

c) Crea alguna regla en la DMZ para publicar algún servicio en la DMZ y que sea accesible desde Internet por la dirección pública del router.

4. Servidores proxy

Es evidente que no todos los ordenadores de una red pueden estar directamente en Internet. Cada host en Internet consume al menos una dirección IP, y ya hemos visto que con el sistema de direccionamiento IPv4 esto no es posible, ya que hay menos direcciones IP disponibles que nodos en Internet.

Por otra parte, no podemos poner un módem u otro acceso a cada estación de la red que tenga acceso a Internet. Lo ideal sería que las conexiones remotas pudieran ser compartidas por varios equipos.

4.1. Características generales

Una aplicación de red especializada para el acceso a Internet desde una red de área local es el **servidor proxy,** que se encarga, entre otras funciones, de compartir las conexiones a Internet y de habilitar una memoria caché con las páginas solicitadas por los usuarios de la LAN de modo que los accesos repetidos a la misma página sean mucho más rápidos, salvaguardando el preciado ancho de banda.

Un servidor proxy de un servicio es un intermediario de red entre el cliente que solicita el servicio y el servidor que lo brinda. El cliente solicita el servicio al proxy, quien a su vez gestiona la petición en su propio nombre al servidor de destino.

Aunque el servicio proxy es muy especializado, algunos sistemas operativos de red, incluso de escritorio, incorporan funcionalidades tecnológicamente cercanas al proxy para compartir accesos remotos a Internet en pequeñas redes locales, típicamente domésticas. Es el caso de la tecnología **ICS** (*Internet Connection Sharing*, compartición de conexión a Internet) que Microsoft incorpora en sus sistemas a partir de Windows 98 para redes domésticas, o las tecnologías **NAT** (*Network Address Translation*, traducción de direcciones de red) comentadas en el RFC 1631.

El servidor proxy más común es webproxy (servidor proxy web o simplemente proxy), que permite a una red interna navegar por Internet mediante una única conexión a Internet.

Un servidor proxy enmascara las direcciones IP internas de la red de área local, sustituyéndolas al poner los paquetes en Internet por la suya propia, dirección real y única en el ámbito de Internet. De este modo, el cliente, típicamente un navegador, negocia la petición a Internet con el proxy y este gestiona el acceso a las páginas solicitadas. Cuando el servidor web remoto envía información al proxy, este hace la sustitución inversa en las direcciones IP y envía los datos a la estación que los solicitó. Por tanto, un servidor proxy también cumple con algunas de las funciones de cortafuegos.

4.2. Configuración del proxy

El navegador debe ser configurado correctamente para informarle de que cada vez que quiera realizar un acceso a Internet, no debe hacerlo directamente, sino a través del proxy. Los parámetros de configuración son básicamente dos: la dirección o nombre del proxy que atenderá nuestras peticiones y los puertos que atenderán nuestras peticiones en función de las aplicaciones. En las Figs. 6.12, 6.13 y 6.14 se pueden ver las fichas de configuración de tres navegadores para la utilización de un servidor proxy.

Ampliación

Aunque aquí se ha hablado siempre del servidor proxy como un intermediario entre el explorador de Internet del usuario y el servidor web sobre el que navega, no siempre hay que entender los servicios proxy de este modo, aunque sí es lo habitual. Los servidores proxy lo son de algún servicio en concreto, por ejemplo, existen servidores proxy de DNS que admiten peticiones de resolución de nombres de clientes y las encaminan en su nombre a los auténticos servidores DNS.

En general, cuando se habla de servidor proxy se referirán al servidor proxy web si no se especifica nada más, pero hay que fijarse bien porque a veces los servidores proxy llevan apellido.

CEO

SMR_RL_AAbad_06_EjemploIPCOP.docx

Documento que contiene información sobre un ejemplo de cortafuegos corporativo IPCOP.

CEO

SMR_RL_AAbad_06_EjemploNetBoz.docx

Documento que contiene información sobre un ejemplo de cortafuegos corporativo NetBoz.

Investigación

Un proxy transparente es aquel que proporciona servicios a sus clientes sin necesidad de una configuración especial, pero a cambio requiere que la red esté configurada de una manera específica. Por ejemplo, como el navegador no tendrá configurada su ficha de proxy, las peticiones se harán siempre a la puerta por defecto, que debe coincidir siempre con el servidor proxy «transparente» que admita peticiones directas del navegador.

Investiga en Wikipedia por la voz «proxy»: qué se entiende por proxy transparente y para qué se utiliza.

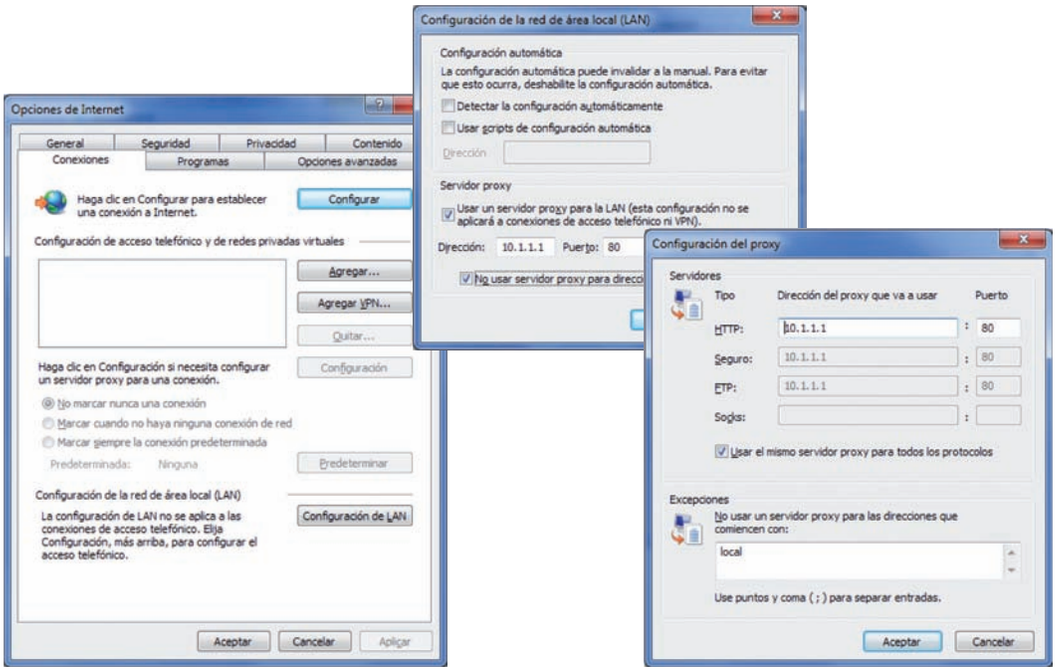
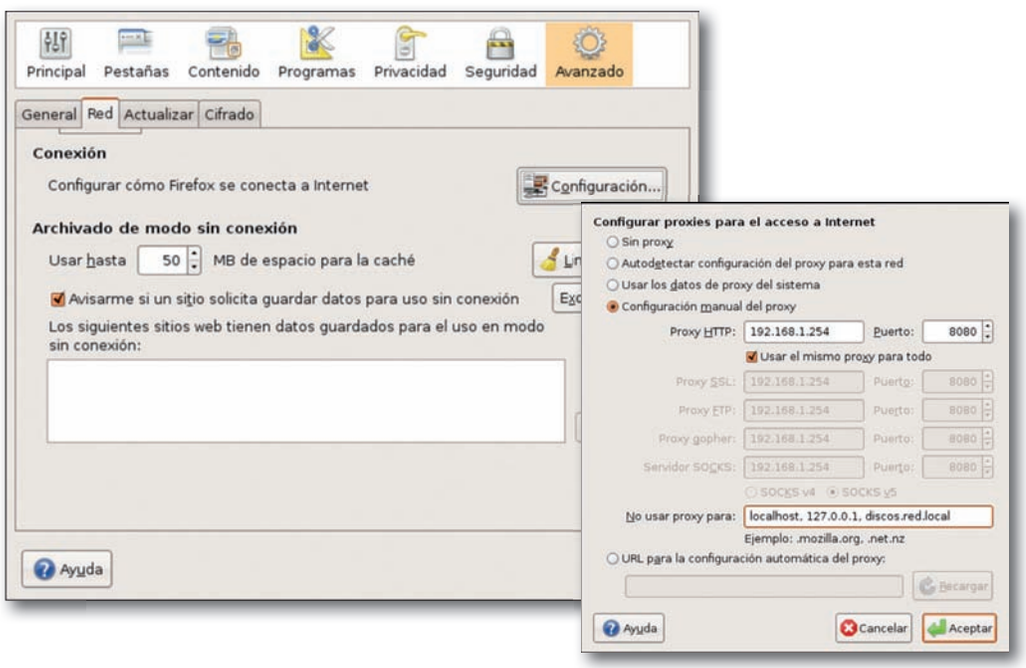


Fig. 6.12. *Fichas de configuración del navegador Internet Explorer para el acceso a través de servidor proxy.*

Por otra parte, el servidor proxy debe estar correctamente configurado. La información típica de configuración de un servidor proxy consiste en el conocimiento de las líneas de comunicación que puede habilitar en caso de necesidad (por ejemplo, a través del marcado automático), los usuarios que tendrán derecho de acceso a Internet, posibles filtros de contenidos, configuración de la memoria caché de páginas, etc.

En Firefox se puede configurar el proxy accediendo al menú *Editar* en la opción *Preferencias*. Desde allí podemos elegir la pestaña *Red* (figura de la izquierda). El botón de *Configuración* permitirá abrir la ventana de *Configurar proxies para el acceso a Internet* (figura de la derecha).



Hemos configurado que el proxy http está en 192.168.1.254 y atenderá peticiones por el puerto 8080. Este proxy http también puede resolver las peticiones del resto de los protocolos: ssl, ftp, etc.

Por último, le indicamos al navegador que no utilice proxy cuando tenga que acceder a algunas direcciones, que se supone que se alcanzarán en local o a través de alguna de las rutas de red: localhost (el propio nodo), 127.0.0.1 (también el propio nodo, alcanzable por la dirección de *loopback*) y el servidor discos.red.local.

Fig. 6.13. *Fichas de configuración del navegador Firefox sobre Linux para el acceso a través de servidor proxy.*

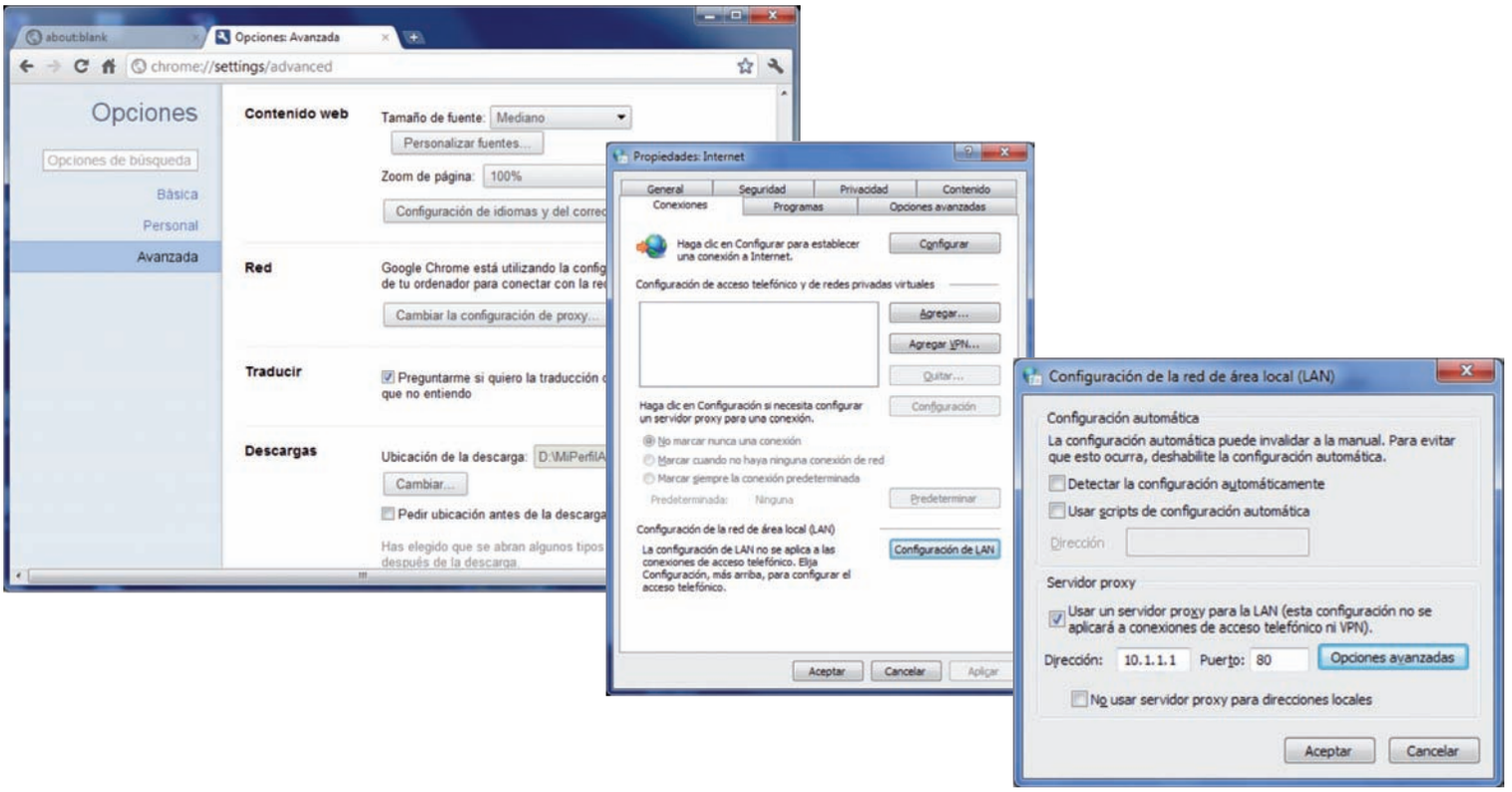


Fig. 6.14. *Fichas de configuración del navegador Google Chrome sobre Windows para el acceso a través de servidor proxy.*

Actividades

12. ¿Cuáles de las afirmaciones siguientes son erróneas?

a) El protocolo NAT traduce los números de puertos entre la red externa y la interna.

b) Cuando se utiliza NAT las direcciones privadas quedan ocultas a la red externa.

c) Hay que elegir entre traducir direcciones o traducir puertos, pero no se pueden traducir ambos simultáneamente.

d) Dos proxies web pueden encadenarse siempre y cuando no utilicen NAT.

e) Todos los enrutadores que tienen acceso a Internet deben configurar NAT en la red externa.

13. Descubre dónde están los errores en el siguiente razonamiento:

«Un servidor proxy atiende peticiones web por la dirección 10.1.20.15 y el puerto 80. Este proxy web está encadenado a otro, utilizando NAT, con dirección 10.1.30.1 por el puerto 8080, que ya no usa NAT para salir a Internet. Un cliente de la red tiene por dirección IP 10.1.20.100 con máscara 255.255.255.0 y sin puerta por defecto. Como el segundo proxy no utiliza NAT el usuario ha decidido configurar su ficha de proxy en el navegador apuntando a 10.1.30.1 por el puerto 8080, que es por el que escucha el segundo web proxy. Después el usuario prueba la navegación, pero no le funciona».

14. Preséntate en una máquina Windows y modifica los parámetros de configuración del proxy en Internet Explorer.

a) Configura el navegador para utilizar el proxy 192.168.201.254 por el puerto 8080 para todos los protocolos que admite el navegador.

b) Configura ahora el navegador para utilizar el proxy anterior, pero solo para los protocolos http y ftp.

15. Repite el ejercicio anterior sobre una estación Linux con navegador Firefox. Si no dispones de esta estación, puedes descargar una versión de Firefox sobre Windows desde **http://www.mozilla-europe.org/es/firefox/**

16. Vuelve a repetir la operación del ejercicio anterior con Google Chrome, que se puede descargar desde **http://www.google.es/chrome**

Caso práctico 1

Configuración de red de un equipo portátil para utilizar varios proxies

Supongamos que una empresa contrata un servicio de auditoría y el auditor se incorpora temporalmente a la empresa para llevar a cabo su función en donde conectará su portátil. La instalación de red de la empresa, por seguridad, tiene prohibida la navegación web, sin embargo, los trabajadores necesitan ftp para cargar y descargar ficheros de un servidor en Internet. Para ello, el administrador ha contratado los servicios de un proxy ftp en la dirección 192.168.120.55 por el puerto 8008. Los clientes habituales no pueden modificar ni la configuración de sus navegadores ni sus direcciones IP, de modo que la seguridad está relativamente garantizada.

El auditor, en cambio, sí necesita acceder a la web mediante protocolo http y el administrador de red ha resuelto instalar temporalmente un servidor proxy local en 192.168.1.101 por el puerto 8080. Cuando el auditor acabe su tarea, el administrador dará de baja el web proxy y todo volverá a ser como antes, puesto que nada más en la red se ha modificado para habilitar temporalmente este servicio.

La red local tiene un servidor DHCP que le ha dado al portátil del auditor la dirección 192.168.1.20/24 con puerta por defecto 192.168.1.254, que es el enrutador hacia Internet.

Vamos a estudiar cómo el administrador de red tiene que configurar el navegador del auditor y qué ruta siguen los paquetes cuando se utiliza el protocolo http y el ftp.

Para configurar correctamente el servidor proxy del portátil del auditor, deberemos tener en cuenta que el servidor proxy ftp debe apuntar al servidor ftp de la empresa (utilizará para ftp los mismos servicios de red que el resto de los empleados: 192.168.120.55 por el puerto 8008), mientras que para el resto de los protocolos se hace apuntar el navegador al nuevo proxy (192.168.1.20 por el puerto 8080).

Ahora vamos a estudiar qué ruta siguen los paquetes http y ftp fijándonos en el diagrama de la Fig. 6.15.

Protocolo http

Cuando el auditor quiere acceder a una página web (accesible mediante el protocolo http), la configuración de su navegador le indica que debe recurrir al servidor web proxy 192.168.1.101 por el puerto 8080. Como 192.168.1.101 está en la misma red IP que el portátil del auditor (cuya dirección es 192.168.1.20/24), el proxy se alcanza sin necesidad de ningún enrutamiento y la conexión es directa (paso A).

Una vez que la petición esté en el proxy web este mandará la petición al encaminador corporativo (paso B) que es quien sabe salir a Internet, en donde estará situado el servidor web solicitado (paso C).

Protocolo ftp

En este caso la configuración del proxy dice que hay que acudir al proxy ftp situado en 192.168.120.55 por el puerto 8008, pero esta dirección no está en la red local, que es la red 192.168.1 (en donde están el portátil del auditor y el puerto LAN del enrutador corporativo). Entonces, para enviar este paquete hay que pasar antes por el encaminador (paso D), que sabrá llegar a la dirección 192.168.120.55 que es donde está el proxy ftp (paso E) y este a su vez reencaminará la petición al servidor ftp solicitado, utilizando los mecanismos de enrutamiento disponibles para su salida hacia Internet, lo que dependerá de la dirección IP del destino, posiblemente pasando de nuevo por el enrutador corporativo.

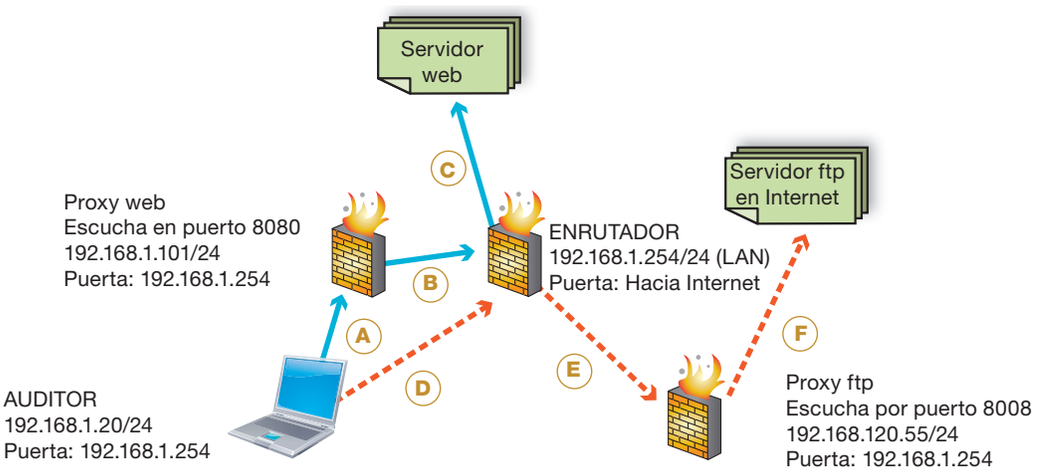


Fig. 6.15. *Ruta de los paquetes http (línea continua) y ftp (línea discontinua) desde el portátil del auditor.*

Caso práctico 2

Configuración de un equipo para mejorar el servicio utilizando un webproxy

Los servicios webproxy pueden proporcionar cierto valor añadido. Esto se consigue si en el proceso de convertir sus entradas desde Internet hacia las salidas en la LAN se introduce un nuevo paso que aporte valor al proceso.

Por ejemplo, si estamos descargando un fichero, el webproxy podría encargarse de hacer un test al fichero y comprobar si está infectado por algún virus.

Esto quiere decir que los servicios de descarga, típicamente http y ftp, deberían modificar su trayectoria de comunicación hacia Internet haciendo que los navegadores tengan configurado un servidor proxy con esta capacidad antivirus con estos dos servicios. La mayor parte de los antivirus comerciales analizan el tráfico de navegación de los clientes en donde se instalan por este procedimiento.

En este caso la configuración del proxy en el navegador de un usuario de la red tendría que tener el aspecto de la Fig. 6.16.

Algunos otros ejemplos de procesos proxy con valor añadido son:

- Chequeo de spam en correo electrónico para servidores proxy SMTP y POP.
- Chequeo de antivirus para correo electrónico para servidores proxy de correo.
- Filtrado de direcciones web sobre servidor proxy.

CEO

SMR_RL_AAbad_06_ConfiguracionProxies.pptx

Documento que contiene información sobre figuras de configuración de diversos servicios proxy con valor añadido como filtrado de spam o antivirus.

Se puede ver que el proxy lleva configurados exclusivamente los dos servicios que serán tratados por el antivirus: http y ftp, que apuntarán a la dirección 192.168.15.2 por el puerto 8080 que es donde supuestamente debe recoger las entradas en proxy que incorpora la aplicación antivirus.

El resto de protocolos saldrán por la ruta normal de salida: habitualmente la puerta por defecto del equipo.

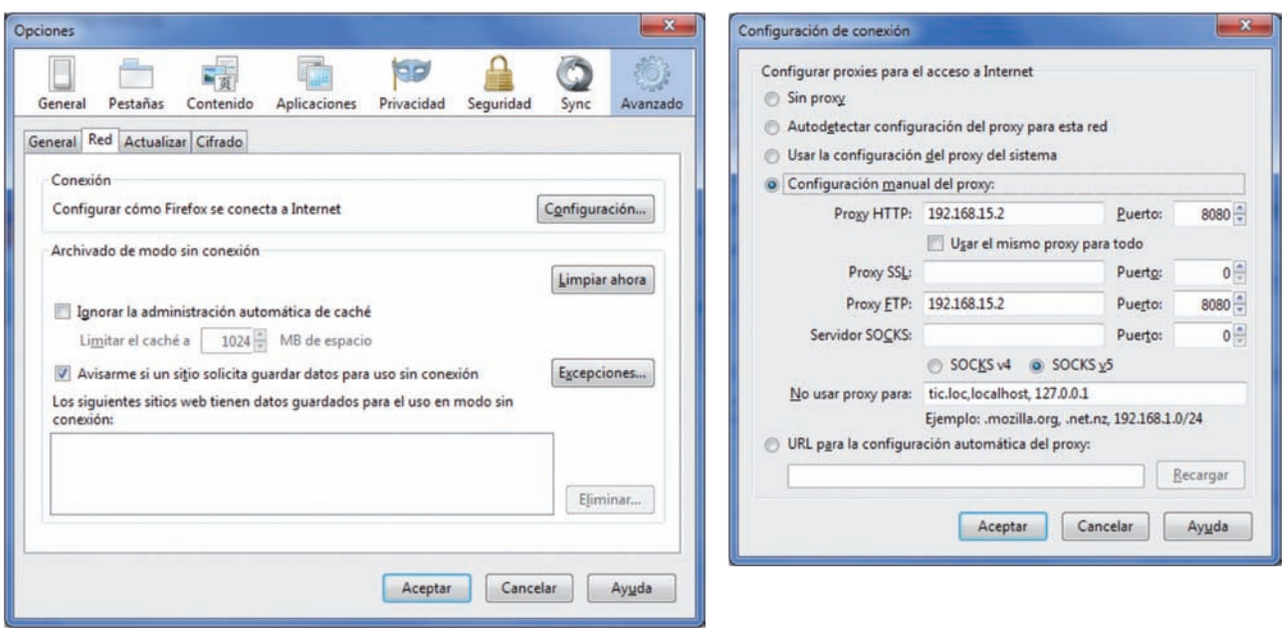
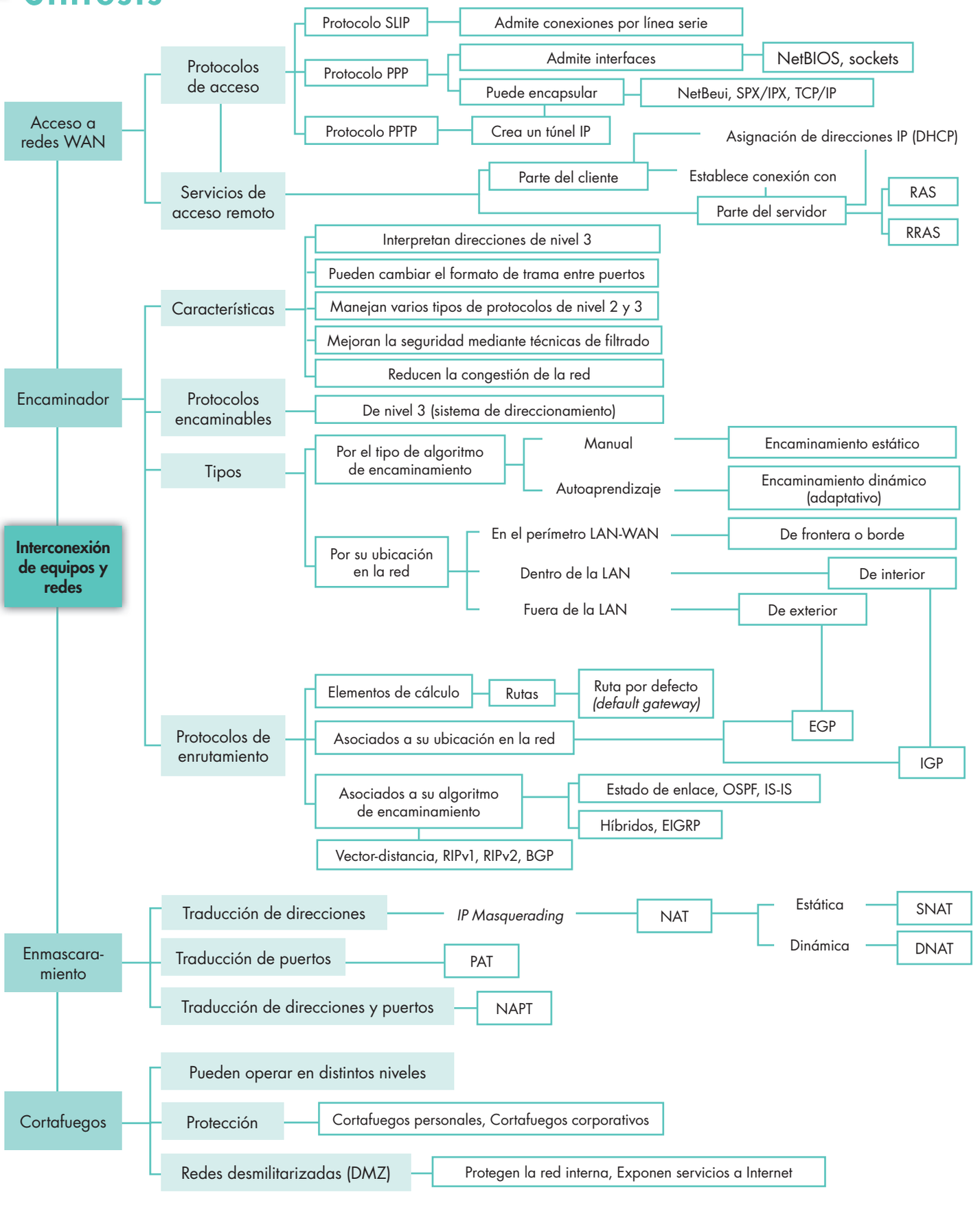


Fig. 6.16. *Configuración del navegador Firefox para una redirección de servicios http y ftp.*

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de algunas de las tecnologías de acceso a redes:

a) PPTP/SLIP	1) Servidor de acceso
b) RAS/RRAS	2) Acceso sobre ATM
c) PPPoE	3) Acceso sobre Ethernet
d) PPPoA	4) Protocolo de acceso remoto

2. El encaminador…

a) Opera en el nivel 3 de OSI.

b) Enruta paquetes NetBIOS.

c) Enruta paquetes IP.

d) Enruta segmentos TCP.

e) Enruta tramas Ethernet.

3. Asocia los siguientes protocolos de enrutamiento con el tipo de tecnología que usan en su algoritmo de encaminamiento:

a) RIPv1	1) Híbrido
b) RIPv2	2) Estado de enlace
c) IGRP	3) Vector distancia
d) OSPF	
e) EIGRP	

4. Cuáles de las siguientes afirmaciones son verdaderas:

a) Un router de exterior solo puede ejecutar algoritmos de encaminamiento estático.

b) Un router de interior solo puede ejecutar algoritmos de encaminamiento estático.

c) Un router de interior puede ejecutar cualquier tipo de algoritmo de encaminamiento, tanto estático como dinámico.

d) Los routers de frontera no pueden ejecutar algoritmos de encaminamiento.

5. Asocia las características de los protocolos de traducción siguientes:

a) NAT	1) Asignación estática de direcciones públicas
b) PAT	2) Traducción de puertos
c) DNAT	3) Asignación dinámica de direcciones públicas
d) SNAT	4) Traducción de puertos y direcciones
e) NAPT	5) Traducción de direcciones

6. La orden **ROUTE ADD –P 192.168.201.0 MASK 255.0.255.0 192.168.1..254**

a) Es incorrecta porque hay un problema en la máscara.

b) Es válida en Windows, pero no en Linux.

c) Es totalmente correcta en Windows.

d) Si fuera correcta, añadiría una ruta permanente.

7. Una red DMZ…

a) Proporciona un segmento de red desmilitarizado que no puede sufrir ataques.

b) Expone algunos servidores hacia Internet protegiendo la red interna.

c) No tiene comunicación con la red interna.

d) Impide la comunicación de sus nodos con Internet.

8. Relaciona las órdenes que aparecen en la columna de la izquierda con los sistemas operativos que se indican en la columna de la derecha.

a) ip route add	1) Windows
b) route add	2) Linux
c) route delete	
d) iptables	
e) ip route	
f) route print	

9. El cliente que accede a Internet a través de un webproxy no transparente:

a) Basta con que configure en el navegador la dirección IP del webproxy.

b) Basta con que configure en el navegador el puerto de escucha del webproxy.

c) Necesita configurar en el navegador tanto la dirección IP como el puerto de escucha del webproxy.

d) No requiere de ninguna configuración especial.

10. Un servidor proxy web está configurado como transparente. Según esto, analiza la veracidad de las siguientes afirmaciones para que pueda navegar por Internet:

a) La puerta por defecto del cliente debe apuntar al servidor proxy.

b) La puerta por defecto del cliente tiene que ser lógicamente compatible (estar en la misma subred) con la IP del servidor proxy.

c) Basta con que cliente y servidor sean visibles recíprocamente en el segmento de red local.

d) Necesita configurar en el navegador tanto la dirección IP como el puerto de escucha del webproxy.

Solución: 1: a-4, b-1, c-3, d-2; **2:** a y c; **3:** a-3, b-3, c-3, d-2, e-1; **4:** c; **5:** a-5, b-2, c-3, d-1, e-4; **6:** a, b y d; **7:** b; **8:** a-2, b-1, c-1, d-2, e-2, f-1; **9:** c; **10:** a.

Comprueba tu aprendizaje

I. Configurar los clientes de una red local para utilizar un sistema de enrutamiento

1. Los protocolos PAP y CHAP, entre otros, son protocolos utilizados por RAS para la autenticación de usuarios. Busca información para comprender mejor cómo funcionan. Fíjate de modo especial en si las contraseñas viajan o no encriptadas por redes inseguras. Puedes empezar tu búsqueda por:
   - **http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-ppp.authentication.html**
   - **http://www.tech-faq.com/lang/es/ppp-authentication.shtml**
2. Utiliza la orden de Windows ROUTE PRINT para identificar todas las rutas IP de un nodo conectado a una red TCP/IP. Observa cuál es el destino de la ruta por defecto. Identifica las direcciones IP de las redes y sus máscaras.

   Ahora repite el mismo procedimiento en otras estaciones de la misma red y establece comparaciones entre los resultados obtenidos en cada estación, razonándolas.

   Puedes repetir esta actividad sobre un nodo Linux utilizando la orden **ip route show.**
3. En la dirección web **http://es.wikipedia.org/wiki/Enrutador** puedes encontrar una información detallada de las características técnicas, protocolos y procedimientos de routers para acceso de banda ancha. Lee el documento para darte cuenta de cómo se integran todos estos elementos en las propuestas comerciales de los fabricantes de hardware de comunicaciones. Acude después a la sede web de algún fabricante de routers para contrastar el documento que has leído con las especificaciones técnicas concretas de algún modelo de router. Te pueden servir las páginas **http://www.juniper.net/es/es/** o **http://www.cisco.com/web/ES/index.html**
4. ¿Cuáles de las siguientes afirmaciones son verdaderas?
   a) La distancia telemática al destino se mide con un parámetro que se denomina coste de la ruta.
   b) RIPv1 está limitado a 15 saltos, sin embargo la versión RIPv2 supera esta limitación.
   c) OSPF siempre envía el paquete por la ruta más corta según el número de saltos.
   d) EIGRP es un protocolo de enrutamiento híbrido.

II. Gestionar un proxy web

5. Ayudándote de Internet, responde:
   a) ¿Cómo se debe configurar un cliente para que pueda utilizar un proxy transparente?
   b) ¿Para qué utilizan los proveedores de Internet los proxies transparentes?
   c) ¿Sabrías averiguar si tu proveedor de Internet te proporciona el servicio de acceso a través de un proxy transparente?
6. Si resumimos los datos planteados en el Caso práctico 1, tenemos que un cliente de red tiene dirección IP 192.168.1.20/24 y su puerta por defecto es 192.168.1.254. El usuario presentado en ese cliente necesita navegar, pero 192.168.1.254 no tiene un proxy transparente y, por tanto, necesita configurar un servidor web proxy. La red tiene dos servidores proxy, uno para el protocolo ftp en la dirección 192.168.120.55 por el puerto 8008 y otro proxy para el resto de los protocolos en la dirección 192.168.1.101 en el puerto 8080.
   a) Si habilitamos en 192.168.1.254 un proxy transparente de tipo web (solo http), ¿cómo sería la ficha de configuración del navegador?
   b) Ahora en 192.168.201.254 habilitamos también la transparencia para el protocolo https, ¿cómo habría que configurar el proxy?
   c) En el caso c), ¿qué puertos tendría que poner a la escucha el servidor proxy transparente en 192.168.1.254?

III. Diseñar y configurar un sistema de protección para la red local

7. Imaginemos un nodo de la red local que no necesita conectarse a Internet más que para navegar por la web.
   a) Si no puede acceder a un servidor proxy, ¿debe tener configurada al menos la puerta por defecto para poder navegar por la web?
   b) ¿Y si tiene acceso a un servidor proxy que está en la red de área local?
   c) ¿Y si tiene acceso a un servidor proxy que está en otra red?
8. Conecta dos estaciones de trabajo en una misma red de modo que sus parámetros de red hagan sus comunicaciones totalmente compatibles.
   a) Comprueba que desde cada estación puedes acceder a todos los servicios de la otra sin ninguna restricción. Por ejemplo, puedes habilitar servidores web y ftp locales para realizar estas pruebas.
   b) Ahora cierra todas las comunicaciones en una de las estaciones y habilita el cortafuegos personal. Comprueba que ahora no puedes acceder a los servicios a los que antes tenías acceso.
9. En **http://m0n0.ch** puedes encontrar el software y documentación técnica de m0n0wall, un *firewall* sobre Linux FreeBSD con muchas prestaciones.

   Lee la documentación técnica para instalar sobre una máquina un cortafuegos m0n0wall, configúralo para que sea útil en tu red y prueba su funcionamiento. Una alternativa muy interesante a m0n0wall es IPFire, que se puede descargar de **http://www.ipfire.org/**

Unidad 7

Redes mixtas integradas

En esta unidad aprenderemos a:

- Identificar las características funcionales de las redes inalámbricas y su relación con la configuración.
- Identificar los protocolos de cifrado y autenticación utilizados en redes.
- Integrar redes mixtas.

Y estudiaremos:

- Los estándares de redes inalámbricas.
- El sistema de direccionamiento IPv6.
- Los dispositivos de conexión que integran las redes mixtas.

Vocabulario

Red de área local inalámbrica o WLAN *(Wireless Local Area Network):* es una red local que transmite mediante ondas de radio y ofrece dos ventajas sustanciales: no es necesario extender cableado por lugares en los que sería imposible o muy difícil y, por otra parte, admite la movilidad de los ordenadores de la red.

1. Redes inalámbricas

En la actualidad se tiende a pensar que la solución a todos los problemas de bajo nivel de los administradores de red es la implantación de redes inalámbricas, pero no es así: el ancho de banda de la red inalámbrica es significativamente menor que el de las redes de cables y la seguridad, si no se cuida, puede verse seriamente comprometida.

1.1. Tecnologías inalámbricas

Aunque las redes inalámbricas más extendidas actualmente siguen el estándar **Wi-Fi,** existen más redes inalámbricas que las recomendadas por él, por ejemplo las redes de infrarrojos, las HomeRF y las Bluetooth. Exponemos a continuación una tabla comparativa de sus características (Tabla 7.1), aunque solo nos detendremos en Bluetooth y Wi-Fi por ser las más representativas.

	IEEE 802.11b, g, a, n	Bluetooth	HomeRF
Velocidad	11, 54, 54, 600 Mbps	3 a 400 Kbps	1 a 10 Mbps
Ámbito[1]	Redes domésticas (SOHO) y empresariales	Redes personales	SOHO *(Small Office, Home Office)*
Alcance	Hasta 100 metros	10 a 20 metros	50 metros
Soporte	Cisco, Lucent, 3Com, Consorcio WECA	Bluetooth Special Interest Group, Ericsson, Motorola, Nokia	Apple, Compaq, Dell, HomeRF Workgroup, Motorola, Proxim

Tabla 7.1. *Comparativa de algunas tecnologías de redes inalámbricas.*
[1] Las distancias que aquí se especifican son estimativas, pues dependen, entre otros factores, de las características del medio, de la velocidad de transmisión elegida y de la potencia de las antenas.

Fig. 7.1. *Dispositivos inalámbricos. Abajo a la izquierda, teléfono móvil y auricular manos libres conectados a través de Bluetooth.*

A. Bluetooth

Bluetooth es una iniciativa para conseguir intercomunicación inalámbrica entre dispositivos de uso personal: teléfonos móviles, ordenadores portátiles, etc. Utiliza una potencia de transmisión muy baja, por lo que su alcance queda limitado a redes domésticas bajo penalización de la velocidad de transmisión. En transmisiones inalámbricas al alcance de la señal se le denomina formalmente **rango.**

Bluetooth utiliza la banda de frecuencia de 2.4GHz con señalización **FHSS** (*Frequency Hopping Spread Spectrum,* Espectro extendido por salto de frecuencia) en la que la señal salta entre múltiples frecuencias dentro de la banda de acuerdo con un patrón de sincronización conocido exclusivamente por el canal establecido entre emisor y receptor.

Los dispositivos Bluetooth se clasifican de acuerdo con tres clases en función de su potencia de transmisión (Tabla 7.2). Bluetooh está definido en la norma IEEE 802.15 que desarrolla cómo deben ser las comunicaciones en redes personales inalámbricas (WPAN).

CEO

SMR_RL_AAbad_07_EjemploBluetooth.docx

Documento que contiene un ejemplo de utilización de la tecnología Bluetooth.

Clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Rango (aprox.)	Ancho de banda (Mbps)
Clase 1	100 mW	20 dBm	~100 metros	Hasta 1 Mbps
Clase 2	2.5 mW	4 dBm	~25 metros	Hasta 3 Mbps
Clase 3	1 mW	0 dBm	~1 metro	Hasta 24 Mbps

Tabla 7.2. *Clases de dispositivos Bluetooth.*

Para utilizar Bluetooth, un dispositivo debe implementar alguno de los perfiles Bluetooth que definen los servicios que pueden utilizarse en el canal establecido. El establecimiento del canal entre emisor y receptor conlleva la creación de una red ad-hoc entre ellos. Para ello se establecen unos mecanismos de descubrimiento de posibles destinos mediante rastreo del espacio radioeléctrico.

En cuanto a la topología, Bluetooth crea un modelo de redes denominadas piconets, que deben cumplir las siguientes características:

1. Todo enlace Bluetooth debe pertenecer a una piconet que le une con un destino por medio de un canal físico compartido y sincronizado mediante un reloj común y una secuencia de saltos de frecuencia única para ese canal. Uno de los extremos de la comunicación hace de maestro y el otro de esclavo.
2. Es posible la coexistencia de varios canales, cada uno de los cuales tiene su propio maestro, reloj y secuencia de saltos.
3. Un dispositivo maestro solo puede serlo de una piconet, aunque un esclavo puede serlo de varias piconets simultáneamente.
4. Un dispositivo puede ser maestro de una única piconet a lo sumo, pero simultáneamente puede ser esclavo de otra u otras piconets distintas de las que él es maestro.

Ampliación

Las redes inalámbricas Wi-Fi tienen una topología desorganizada en la que existen uno o más núcleos emisores/receptores de señal (puntos de acceso) que se conectan a la red troncal. Cada estación lleva su propia antena con la que se conecta a estos núcleos, proporcionando de este modo continuidad lógica a la red utilizando enlaces a 2,4 GHz, la misma banda que utilizan los hornos de microondas.

Este solapamiento de maestros y esclavos en piconets recibe el nombre de *scatternet* (red dispersa) y, aunque son varias piconets entrelazadas, no tienen definidas capacidades de enrutamiento entre ellas ya que Bluetooth solo define protocolos hasta el nivel 2.

En la Fig. 7.2 se puede ver una red dispersa compuesta por 6 piconets Bluetooth. Vamos a analizar cada una de ellas.

- **Piconet 1:** N1 es el maestro. N2, N3 y N4 son esclavos de N1.
- **Piconet 2:** N4 es esclavo de N5, que es su maestro en Piconet 2, aunque N5 es esclavo respecto de N6 en la Piconet 3. N5 es esclavo.
- **Piconet 3:** N6 es maestro. N5 y N7 son esclavos de N6.
- **Piconet 4:** N8 es maestro. N9 es esclavo.
- **Piconet 5:** N11 es maestro de N10 respecto de la Piconet 5, aunque también es esclavo de N12 respecto de la Piconet 6. N10 es esclavo de N11.
- **Piconet 6:** N12 es maestro. N11 es esclavo.

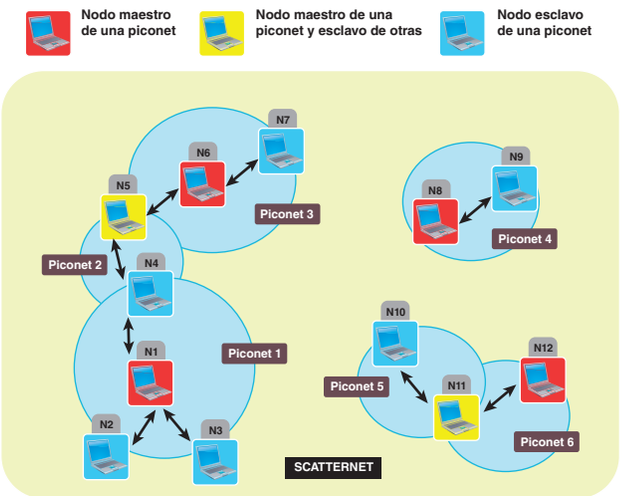


Fig. 7.2. *Representación de una* scatternet *compuesta de múltiples piconets.*

B. Redes Wi-Fi

Las redes inalámbricas existen desde hace años, pero con grandes limitaciones. Se trataba de sistemas propietarios y velocidades de transmisión por debajo de 1,5 Mbps, lo que era claramente insuficiente para una red de área local. En la actualidad la WECA (*Wireless Ethernet Compatibility Alliance,* Asociación de fabricantes de productos Ethernet inalámbricos) extiende certificaciones de compatibilidad (llamadas Wi-Fi) entre dispositivos IEEE 802.11b.

IEEE 802.11 es el estándar propuesto por la IEEE para redes de área local inalámbricas, en el que se define un modo de seguridad básico como elemento de privacidad denominado **WEP** *(Wired Equivalent Privacy),* llamado así porque proporcionaba una seguridad equivalente a la obtenida en redes cableadas sin encriptación.

WEP es un protocolo que presenta un método de cifrado que se aplica a todos los mensajes que circulan por la red. La clave de encriptación debe ser conocida por todas las estaciones y por el punto de acceso. Solo quien posee la clave correcta es capaz de descifrar mensajes. Sin embargo, WEP es una protección muy débil que fácilmente se puede romper, especialmente si se eligen claves de encriptación de 40 bits en vez de 128 bits. La debilidad de WEP ha hecho que la IEEE se plantee la ampliación del estándar utilizando mecanismos de seguridad más fuertes, como los especificados en IEEE 802.1i y la seguridad por puertos IEEE 802.1x.

Seguridad

De modo predeterminado, WEP viene deshabilitado en la mayor parte de los productos comerciales, por lo que hay que tener mucho cuidado cuando se instalan por primera vez dispositivos inalámbricos. Antes de realizar las conexiones de red, WEP debe ser habilitado y configurado correctamente.

Vocabulario

Punto de acceso o **AP (Access Point):** es el dispositivo que centraliza las comunicaciones inalámbricas. Aunque no es imprescindible, suele hacer de integrador entre la red cableada y la red inalámbrica.

Canal de transmisión de una LAN: es un parámetro que especifica la frecuencia a la que se transmitirán las señales entre emisor y receptor, y en la que previamente ambos se han puesto de acuerdo.

Roaming: es la función de los sistemas inalámbricos formados por varias celdas por la que un cliente que se desplaza cambia de celda en celda, buscando la mejor cobertura, sin perder la conexión a la troncal de la red a la que se conectan todas las celdas.

La operativa de funcionamiento de una Wi-Fi consiste en que el punto de acceso transmite una trama de administración que contiene un identificador único **SSID** *(Service Set Identifier)* o **BSSID** *(Basic SSID)*. El valor de SSID se establece en tiempo de configuración del punto de acceso.

La estación inalámbrica cliente escuchará esta trama de administración e identificará al punto de acceso. El cliente elegirá un punto de acceso de todos los que ve y establecerá una asociación con él si la negociación de autenticación tiene éxito. A partir de ese momento, el cliente inalámbrico comunicará con otras estaciones a través del punto de acceso, que hará de puente entre los distintos segmentos de red y el resto de estaciones inalámbricas asociadas con él.

IEEE 801.11 establece dos métodos de autenticación o de autorización: **sistema abierto** y **clave compartida.** En el primer caso, cualquier estación puede asociarse al punto de acceso sin más que emitir una solicitud que siempre será aceptada. En el segundo caso, la autenticación será correcta si el cliente sabe la clave secreta, justamente la clave WEP, que deben compartir punto de acceso y cliente.

Muchos puntos de acceso inalámbricos permiten la configuración de filtrado por dirección MAC, es decir, solo los equipos que posean las tarjetas de red cuya dirección MAC esté registrada en el punto de acceso podrán efectuar transmisiones. Esto es muy interesante, pero desgraciadamente es una seguridad muy débil puesto que basta con asignar una dirección MAC de las registradas en el punto de acceso a la tarjeta de red para poder saltarse la protección: la única dificultad estaría en averiguar una de las direcciones MAC registradas.

En cuanto a las técnicas de modulación utilizadas en Wi-Fi, son variadas. Las más utilizadas son **DSSS** *(Direct-Sequence Spread Spectrum)* y **FHSS** *(Frequency Hopping Spread Spectrum)* con diversas variantes en función del estándar elegido.

C. El estándar WiMAX

Vocabulario

Hot spot: es un punto de acceso público al que los clientes inalámbricos acceden bajo ciertas restricciones, como el pago previo del servicio. Es una instalación muy típica de lugares públicos como aeropuertos, recintos feriales, hoteles, etc.

WiMAX es el nombre por el que se conoce a las redes inalámbricas que siguen el estándar **IEEE 802.16** aún en estudio y que define una especificación para redes metropolitanas inalámbricas de banda ancha que pueden llegar hasta los 66 GHz. Realmente WiMAX es el nombre del foro constituido por muchos de los fabricantes interesados en la especificación, a la cabeza de los cuales están Intel y Nokia. Podemos decir que Wi-Fi es a la IEEE 802.11 lo que WiMAX a la IEEE 802.16.

Comercialmente, en redes Wi-Fi se han establecido unos **puntos de acceso** públicos o **hot spots** que reciben las peticiones de clientes Wi-Fi para su acceso a Internet. El cliente queda identificado normalmente a través de una tarjeta o algún procedimiento de autenticación similar. Es un servicio que suele ofrecerse en aeropuertos, hoteles, centros de convenciones, estaciones de transportes y lugares que en general tienen un elevado tráfico de personas. La conexión de estos hot spots a Internet se realiza a través de cable.

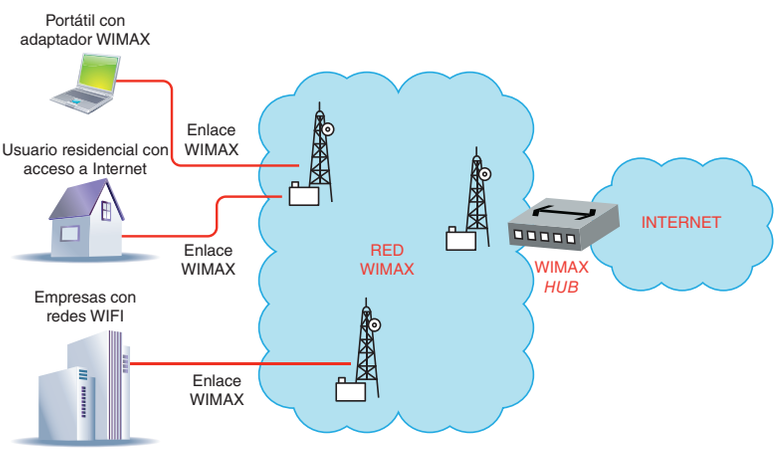


Fig. 7.3. *Configuración típica de una red inalámbrica para su acceso a una red cableada.*

WiMAX es muy interesante para los operadores porque permitiría, entre otras muchas aplicaciones, conectar estos puntos de acceso públicos a Internet sin necesidad de cables, ya que los hot spots accederían a Internet a través de IEEE 802.16, proporcionando servicio de acceso a los clientes inalámbricos a través de IEEE 802.11. El competidor natural de WiMAX es un estándar que empezó a desarrollar sus trabajos en el año 2002; se trata del IEEE 802.20, especialmente indicado para clientes móviles hasta 250 km/h. Como este estándar está aún muy poco desarrollado y la industria ha empezado a apoyar fuertemente al IEEE 802.16, omitimos aquí su desarrollo.

Puede conseguirse abundante información sobre WiMAX a partir de la página **http://es.wikipedia.org/wiki/WiMAX** y de **http://recursostic.educacion.es/observatorio/web/es/equipamiento-tecnologico/redes/349-andres-lamelas-torrijos**

Ampliación

Topologías de conexión en redes inalámbricas

En redes WLAN se definen dos tipos de topologías básicas o modos de conexión. La topología aquí se refiere más bien a los modos en que se puede construir la arquitectura de conexiones de la red, que básicamente son dos: modo ad hoc o punto a punto y modo de infraestructura.

Modo topológico ad hoc

En esta topología, dos nodos cualesquiera pueden comunicarse entre sí después de una etapa de negociación sin necesidad de ningún intermediario. Suele utilizarse para la comunicación entre dos PC o entre un PC y un pocket-PC o para redes pequeñas en las que es fácil establecer conexiones punto a punto. Por ejemplo, Bluetooth y la transmisión por infrarrojos utilizan también este modo de conexión.

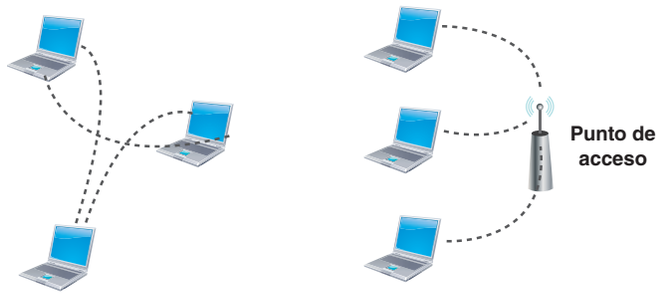


Fig. 7.4. *A la izquierda, modo topológico ad-hoc. A la derecha, topología en infraestructura.*

Modo topológico de infraestructura

En este modo, cuando dos nodos quieren comunicarse entre sí, lo hacen a través de un intermediario que organiza la comunicación entre todos los nodos inalámbricos de la red, que se denomina **punto de acceso** (AP, *Access Point*) o **estación base** *(base station)*. El punto de acceso puede alcanzar a cualquier cliente que esté en su radio de acción, definiendo por tanto una celda semejante a las de telefonía móvil.

Una gran superficie se puede cubrir con varias celdas, cada una de las cuales transmite en un canal determinado.

Geográficamente, no se pueden solapar celdas que transmitan en el mismo canal. El número de canal de transmisión es uno de los parámetros que deben configurarse en los puntos de acceso antes de ponerlos en producción.

El punto de acceso (Fig. 7.4) puede llevar puertos de red no inalámbricos y, de este modo, conectarse a la infraestructura cableada de la instalación, haciendo las veces de puente entre el segmento de red inalámbrico y los segmentos cableados. Este es el modo de conexión habitual utilizado en las instalaciones de red comerciales, formando una red mixta entre la red cableada y la red inalámbrica.

En algunos casos, al punto de acceso se le añaden funciones de conmutación y de enrutamiento, por ejemplo, la mayor parte de los routers ADSL en la actualidad son enrutadores y puntos de acceso Wi-Fi.

Autenticación y cifrado avanzado en Wi-Fi

WEP es un protocolo muy débil cuya encriptación puede romperse con gran facilidad. Para mejorar este aspecto de las redes inalámbricas se inventó **WPA** *(Wi-Fi Protected Access)*, que es una versión muy mejorada de WEP en la que la gestión de claves es dinámica, lo que dificulta una posible labor de ataque.

Más recientemente se ha implantado **WPA2,** basada en el nuevo estándar IEEE802.11i, que todavía mejora WPA y que es la base para las nuevas redes inalámbricas de gran velocidad con gestión de múltiples antenas (tecnología **MIMO,** *Multiple-Input Multiple-Output*).

Actualmente se comercializan productos inalámbricos bajo el estándar IEEE 802.11n, que incorpora muchas y muy nuevas tecnologías de cifrado, radiación y seguridad en la conexión. Lo más significativo de esta tecnología es que realiza las emisiones utilizando varias antenas, mejorando el ancho de banda y la cobertura de radiación. Las redes IEEE 802.11n se basan en el estándar de seguridad IEEE 802.11i.

Fig. 7.5. *Arriba, diferentes tarjetas de red con distintos modelos de interfaz de conexión: USB, PCMCIA y PCI. En el centro, logotipo identificador de la tecnología Wi-Fi. Abajo, puntos de acceso con especificación del fabricante sobre el modo de conexión a la red cableada.*

Ampliación

Muchos dispositivos en la actualidad traen Wi-Fi incorporado: pocket-PC, tablet-PC, teléfonos móviles, etc. También es muy común que los enrutadores de acceso a Internet a través de ADSL incorporen un punto de acceso de modo que los PC que tengan que acceder a Internet salgan a ella a través del punto de acceso del enrutador.

1.2. Tipos de WLAN

Existen varios tipos de WLAN IEEE 802.11. El más común es el establecido por la norma IEEE 802.11b, que utiliza la banda de frecuencia de 2,4 GHz para hacer WLAN hasta 11 Mbps, utilizando modulación DSSS en la capa física. Esta red es lo que denominamos Wi-Fi en sentido estricto.

Una velocidad de 11 Mbps es insuficiente para compartir entre todas las estaciones clientes, por ello se propuso el estándar IEEE 802.11g, que utilizando la misma banda de frecuencia es capaz de llegar a 54 Mbps, aunque algunas compañías tienen productos que alcanzan los 108 Mbps fuera del estándar. Los puntos de acceso IEEE 802.11g suelen ser compatibles con IEEE 802.11b, de modo que pueden recoger señales procedentes del estándar inferior.

El estándar IEEE 802.11a también es capaz de llegar a los 54 Mbps, pero a una frecuencia de 5 GHz. Al ser la frecuencia mayor, la distancia a la que llega es menor; sin embargo, permite un mayor número de canales de comunicación simultáneos.

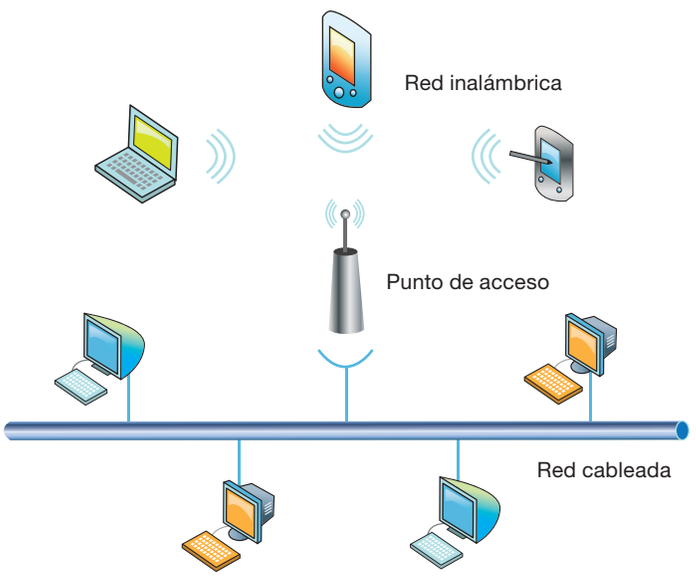


Fig. 7.6. *Configuración típica de una red inalámbrica para su acceso a una red cableada.*

La distancia máxima entre el punto de acceso y la estación inalámbrica varía en función de los obstáculos que encuentren las señales de radio. Además, a mayor distancia, menor será la velocidad de transmisión. A veces hay que instalar antenas especiales con objeto de mejorar la potencia de radiación. Aunque depende de la tecnología utilizada y de muchos otros factores, esta distancia no suele superar los 100 metros, lo que es perfectamente válido para el ámbito doméstico o para el entorno de una oficina. A partir de estas distancias ya tendríamos que diseñar redes especiales en donde unos puntos de acceso hacen de puentes a otros puntos de acceso.

Hay compañías que comercializan sistemas inalámbricos que permiten que múltiples puntos de acceso se gestionen desde una única consola cuando todos ellos están conectados a un **conmutador inalámbrico.** Este es el método elegido para la instalación inalámbrica en grandes corporaciones.

Cuando haya que cubrir instalaciones muy extensas, tendremos que poner muchos puntos de acceso. En Wi-Fi, y también en 802.11g, solo se pueden configurar tres canales de comunicación totalmente independientes, cada uno de los cuales deberá ser utilizado por los puntos de acceso contiguos. A partir del cuarto punto de acceso tendremos que repetir el canal, lo que puede producir interferencias con el primer punto de acceso, pues utilizará el mismo número de canal.

Ejemplos

En la Fig. 7.7 vemos un ejemplo de las celdas de radiación de los puntos de acceso. Los puntos de acceso que utilizan el canal 1 no deberán escucharse entre sí, lo que será posible si se ajusta bien la potencia de radiación de sus antenas. Una de las razones por las que algunas compañías utilizan 802.11a en vez de la versión b o la g, es que la versión a puede utilizar 8 canales distintos en vez de 3, por lo que se atenúa este problema.

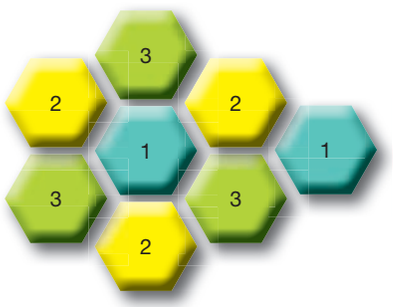


Fig. 7.7. *Mapa de celdas de radiación en Wi-Fi.*

1.3. Integración de Wi-Fi con la red corporativa cableada

Cuando se diseña la instalación de una red no suele empezarse por las conexiones inalámbricas. Normalmente se diseña primero la estructura de cable y los servicios que proveerán los servidores. En una segunda fase se estudian los clientes y su modo de acceso. Si los clientes necesitan movilidad, entonces habrá que diseñar una red inalámbrica que se integre con la parte de red cableada formando una red mixta.

Vamos a estudiar un ejemplo de cómo se integran las redes inalámbricas con el resto de la red. Para ello nos vamos a fijar en la configuración de red propuesta por la Fig. 7.8, que hay que estudiar detenidamente.

En esta red tenemos clientes inalámbricos que se conectan a la red cableada a través de un punto de acceso. En esta red de cable hay un servidor que encamina paquetes entre la LAN cableada y otro router ADSL que proporciona acceso a Internet.

Nosotros, de momento, queremos resolver qué debe ocurrir para que el cliente inalámbrico envíe un paquete al servidor y, en concreto, a la dirección de su interfaz interna (192.168.100.1).

El cliente se pondrá en contacto con su punto de acceso y le enviará las tramas: el único modo que tiene una estación inalámbrica de enviar paquetes a la red en el modo de infraestructura es a través de su punto de acceso. Obsérvese que el punto de acceso está en la misma red que el cliente inalámbrico, en concreto en la red 192.168.100.0/24, aunque esta dirección solo se usa para la gestión del punto de acceso, ya que formalmente un punto de acceso opera en el nivel 2 de OSI. Sería distinto si el punto de acceso tuviera además capacidades de enrutamiento: en este caso su dirección IP sería importante, pero entonces tendría que tener dos, una por cada uno de los dos segmentos que interconectaría.

Una vez que el paquete (encapsulado en tramas IEEE 802.11) llega al punto de acceso, este observa que el destino del paquete está también en su misma red y lo pondrá en la red cableada sabiendo que el servidor lo leerá.

Vocabulario

Conmutador inalámbrico: es un dispositivo especial de la red, normalmente un *switch* avanzado, que permite la gestión centralizada de todos los puntos de acceso de una instalación inalámbrica.

CEO

SMR_RL_AAbad_07_WiMAX.docx

Documento que contiene información sobre redes inalámbricas metropolitanas WiMAX o IEEE 802.16.

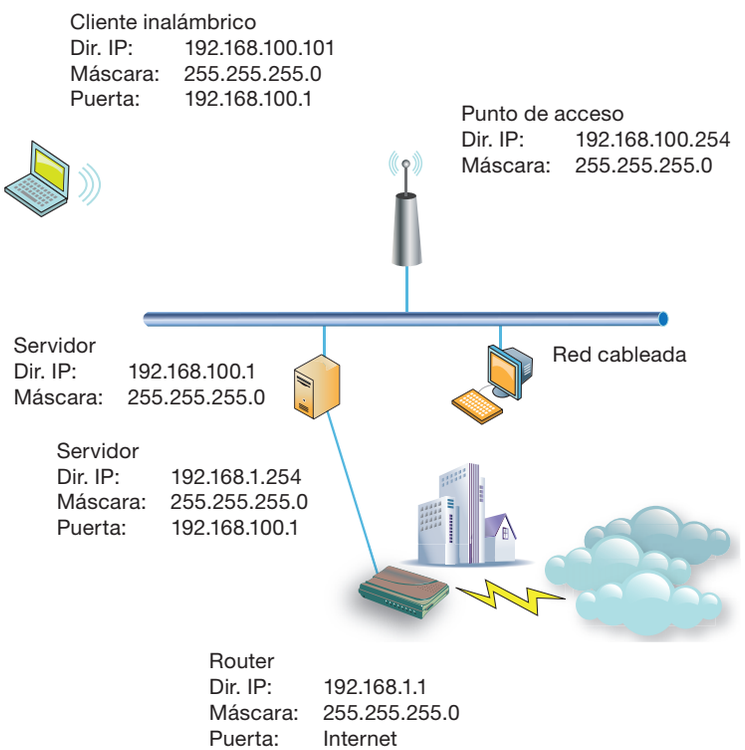


Fig. 7.8. *Mapa de una red inalámbrica integrada con una red cableada.*

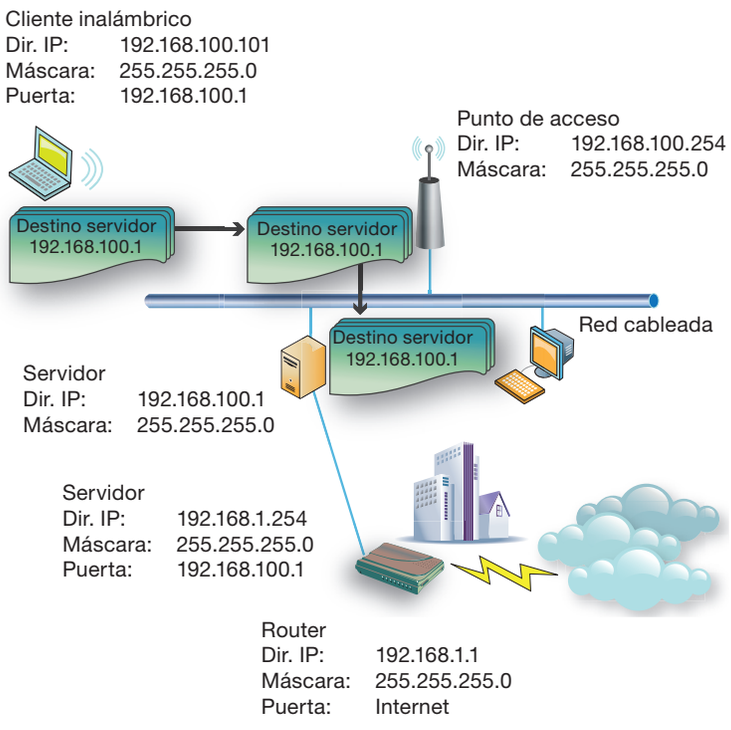


Fig. 7.9. *Solución de envío de paquetes a la LAN.*

Ejemplos

Internetworking

Sobre la misma instalación de la Fig. 7.8, vamos ahora a resolver la salida de un paquete hacia Internet atravesando tanto el servidor de encaminamiento como el router de acceso a Internet (Fig. 7.10). Supondremos que el cliente inalámbrico desea enviar un paquete de datos a la dirección 128.1.25.14, situada en Internet.

Cuando el cliente inalámbrico decide enviar el paquete, lo hace a través del punto de acceso (no tiene otra posibilidad); pero el destinatario del paquete no será el punto de acceso, ya que el destino no se encuentra en su misma red, sino el enrutador, apuntado por su puerta de enlace, que es 192.168.100.1. Enviar un paquete a esa dirección es fácil; de hecho, ya lo hemos logrado en el caso expuesto en la página anterior.

Una vez que el paquete llega al servidor, este se da cuenta de que el destino del paquete (128.1.25.14) no se encuentra en ninguna red conectada directamente a sus interfaces y enviará el paquete a su puerta por defecto, que es 192.168.1.1, justo la dirección IP del router ADSL. Por tanto, el servidor cambiará al paquete de red y lo sacará por la interfaz por donde puede alcanzar al router ADSL.

Una vez que el paquete está en el router ADSL, este enviará el paquete a Internet a través de una jerarquía de rutas definidas en los encaminadores de los proveedores de Internet.

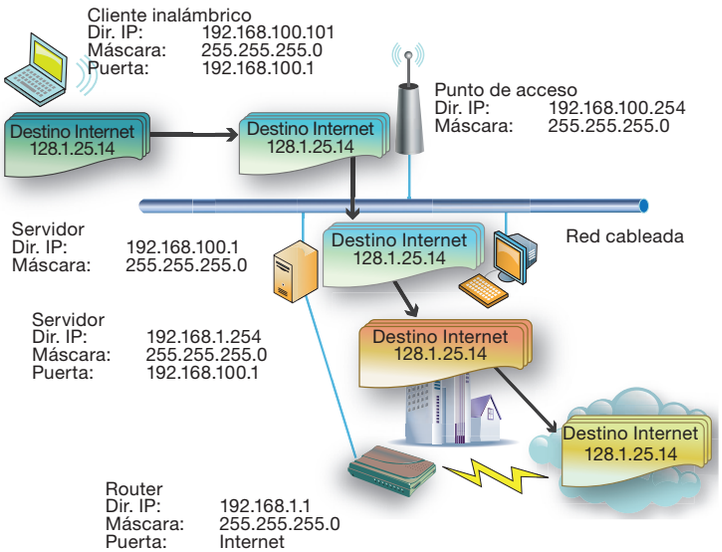


Fig. 7.10. *Solución de envío de paquetes a Internet.*

Caso práctico 1

Configuración de una red inalámbrica Wi-Fi en clientes Windows y Linux

En la actualidad todos los ordenadores portátiles tienen integrada una interfaz de red inalámbrica de tipo Wi-Fi, de modo que se han hecho habituales las conexiones inalámbricas para proporcionar servicio de red a los portátiles. Los administradores de red y, de modo ordinario, todos los usuarios deben conocer el procedimiento de configuración de una tarjeta de red inalámbrica.

Veremos este ejemplo con Windows XP por ser más didáctico. En Windows 7 es mucho más sencillo y se puede hacer siguiendo los pasos que se describen a continuación:

1. En primer lugar habrá que asegurarse de que están instalados los controladores de las interfaces de red inalámbricas.
2. Desde el panel de control del sistema se abre el *Centro de Redes y Recursos Compartidos* y ejecutamos *Conectar a Red.*
3. Aparecerá una lista con todas las redes inalámbricas disponibles. Seleccionaremos una de ellas haciendo clic sobre ella. El sistema pedirá la clave de acceso a la red.

Tomaremos una estación Windows con hardware inalámbrico y configuraremos la tarjeta de red para que se pueda conectar a una red inalámbrica externa.

En primer lugar, exploraremos la ficha de propiedades de la interfaz de red inalámbrica. Para ello, ejecutaremos la ficha de *Conexiones de red* del panel de control de Windows. Seleccionaremos el icono que representa a la interfaz inalámbrica y mostraremos sus propiedades (con el botón derecho del ratón). Nos saldrá algo parecido a la Fig. 7.11.

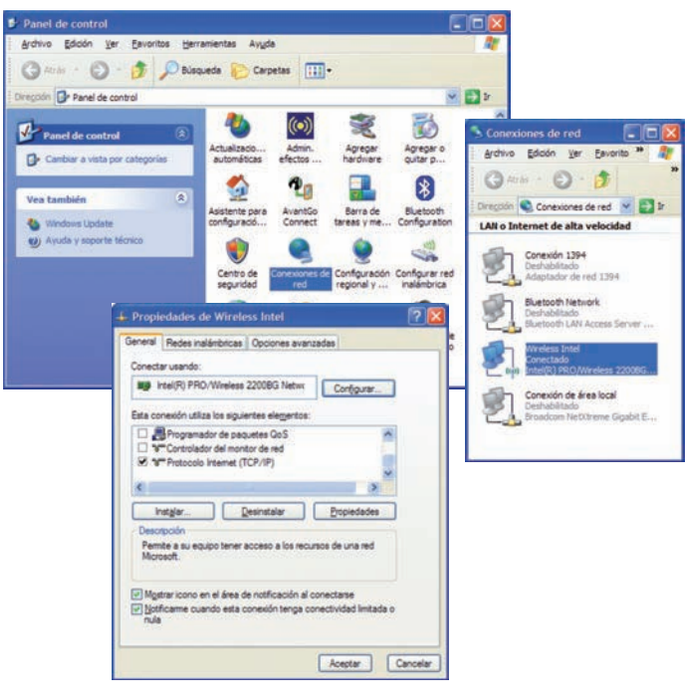


Fig. 7.11. *Secuencia de propiedades de una interfaz inalámbrica en Windows.*

Continúa...

Caso práctico 1

...Continuación

Seguidamente procedemos a configurar la tarjeta de red, es decir, vamos a introducir los parámetros necesarios para conectarnos a la red que deseamos. Ejecutamos el botón *Configurar* y nos aparecerán las fichas propias de Wi-Fi (Fig. 7.12-A).

En el botón de *Opciones avanzadas* podremos seleccionar si las redes que podemos visualizar son redes ad hoc o de infraestructura (Fig. 7.12-C).

En la ficha de *Redes inalámbricas* podremos dar de alta una nueva red inalámbrica o conectarnos a alguna de las que ya existan. En el botón *Ver redes inalámbricas* podremos ver aquellas que estén a nuestro alcance (Fig. 12.9-D), aunque solo nos podremos conectar a ellas si conocemos sus parámetros de comunicación, fundamentalmente la clave y el método de encriptación.

Solicitando una de las redes y pinchando en *Propiedades* podremos escribir o modificar el método de autenticación, el método de cifrado y la clave de red que se utilizará como contraseña de encriptación (Fig. 7.12-B).

Fig. 7.12. *Configuración de los parámetros de una Wi-Fi en Windows.*

Una vez que se han configurado todos los parámetros de la red, la interfaz de red inalámbrica se conectará automáticamente a la Wi-Fi deseada, que se comportará como cualquier otra red.

En el caso de Linux el sistema es muy parecido. Partimos de la configuración de las interfaces de red, que se gestionan desde la misma utilidad gráfica que el resto de interfaces de red (Fig. 7.13-A). Desde allí podremos determinar que queremos el modo itinerante (no deseamos configurar nada, todo será automático) o bien queremos conectarnos a alguna red concreta (asociarse a algún punto de acceso disponible) con unos parámetros adecuados para esa red. En la Fig. 7.13-B vemos la posibilidad de conexión a una red denominada «La Hacienda», cuyo punto de acceso tiene dirección MAC 00:02:6F:20:DF:80 y que no es una red segura (sin encriptación).

Seguidamente elegiremos los ajustes inalámbricos: tipo de encriptación (WEP, WPA, etc.) y otros ajustes de conexión (dirección IP, máscara, puerta de enlace, etc.). Si se activa el modo itinerante, todos estos ajustes serán automáticos y no habrá que rellenarlos (Fig. 7.13-C).

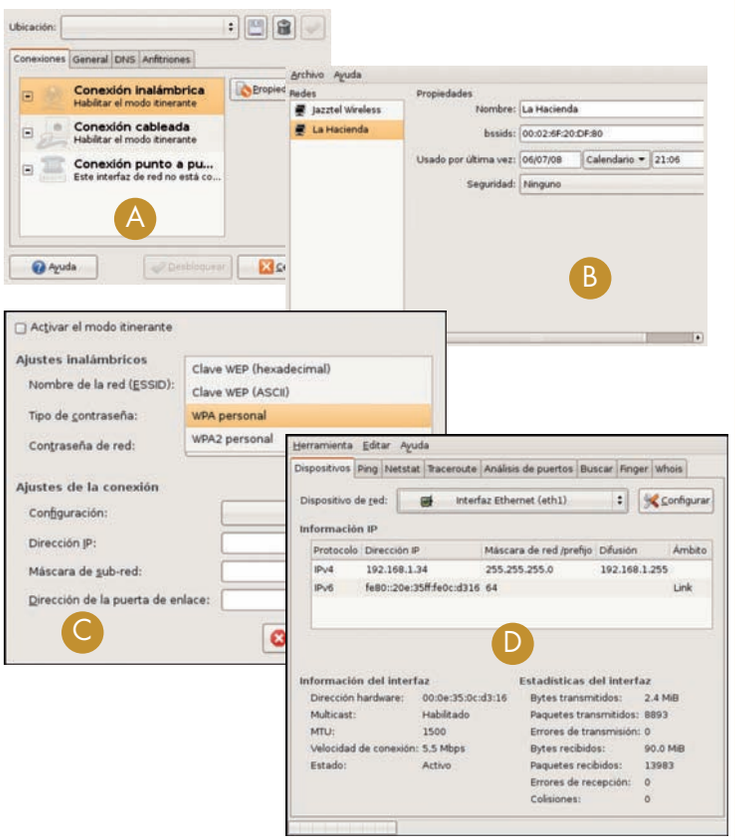


Fig. 7.13. *Configuración de los parámetros de una Wi-Fi en Linux.*

Continúa...

Caso práctico 1

...Continuación

Si una vez suministrados los parámetros se comprueba que son correctos, se procederá a realizar la conexión como si de cualquier otra red se tratara. En la Fig. 7.13-D podemos ver que la red inalámbrica nos ha asignado una dirección IPv4 (192.168.1.34) y que además ha configurado automáticamente una dirección IPv6 de ámbito de enlace (link). En la Fig. 7.14 podemos observar dos ilustraciones, una gráfica y otra textual, que nos permiten comprobar el estado de la conexión.

La orden **iwconfig** es la equivalente inalámbrica de la orden **ipconfig** para las redes de cable. En la Fig. 7.14 podemos ver que se ha realizado una conexión utilizando el estándar IEEE 802.11g, la identificación de la red (ESSID) es «La Hacienda», la frecuencia de radiación de antena es 2.412 GHz y muchos otros parámetros como la dirección MAC del punto de acceso, el nivel de señal en decibelios, etc.

La ilustración gráfica nos proporciona también otros datos complementarios como el sistema de direccionamiento, el controlador de software utilizado por la interfaz inalámbrica, etc.

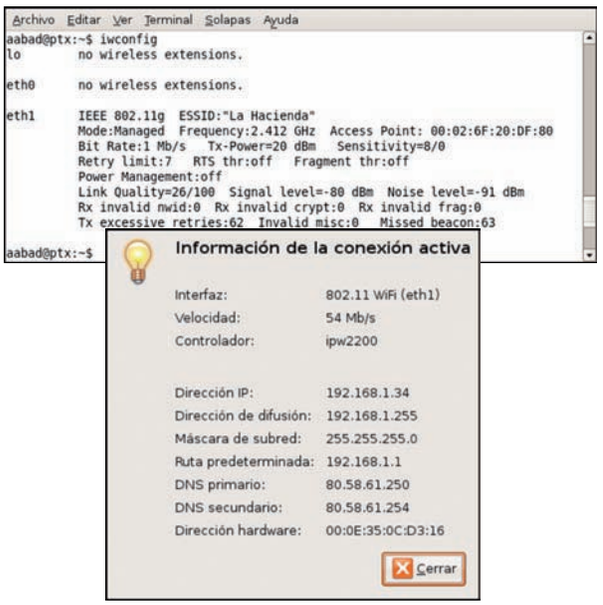


Fig. 7.14. *Comprobación del estado de la conexión en Linux.*

Actividades

1. Relaciona los elementos de la columna de la izquierda con los de la derecha en la siguiente tabla:

Estándar	Característica
IEEE 802.11b	WiMAX
IEEE 802.11g ó a	54 Mbps
IEEE 802.11n	11 Mbps
Bluetooth	PAN
IEEE 802.16	MIMO

2. Descubre los errores en el siguiente razonamiento:

«He configurado un punto de acceso inalámbrico para que los clientes utilicen MIMO como mecanismo de encriptación en sus comunicaciones. Para aumentar la seguridad de la red inalámbrica se ha deshabilitado la publicación del SSID de la red. Cada cliente accederá con su propia clave WEP (distinta para cada cliente) que el administrador de red suministrará a cada portátil inalámbrico».

3. Para realizar este ejercicio necesitarás dos PC clientes Windows con interfaz de red inalámbrica y un punto de acceso. Después, realiza las siguientes operaciones.

a) Configura el punto de acceso para que suministre direcciones IP automáticamente a los clientes inalámbricos.

b) Asigna el canal 6 a la WLAN del punto de acceso (si este canal estuviera ocupado por otro dispositivo puedes elegir cualquier otro canal).

c) Habilita la encriptación WEP de 128 bits (si no estuviera disponible, puedes utilizar la de 64 bits).

d) Configura ahora los dos clientes para que soliciten su dirección IP por DHCP al punto de acceso y se puedan comunicar entre ellos a través de la WLAN.

4. Manteniendo el punto de acceso configurado como en el ejercicio anterior, repite los apartados *c* y *d* sustituyendo los clientes Windows por clientes Linux.

5. Descubre cuál es el problema del usuario que se describe a continuación:

«El usuario de un equipo de sobremesa dispone de un dispositivo USB en cuya superficie el fabricante ha serigrafiado una etiqueta con el texto "USB WiMAX connector". Después de conectar en el puerto USB el adaptador, el usuario ha querido iniciar la conexión a una red IEEE 802.11g que tiene desplegada en su empresa, pero el equipo no encuentra la red y no se puede conectar a ella.»

1.4. Wi-Fi de más de un punto de acceso

Es común que las WLAN incluyan varios puntos de acceso para poder cubrir un mayor rango y para dar soporte a un mayor número de usuarios inalámbricos. Cada punto de acceso puede atender entre 10 y 100 clientes, dependiendo del fabricante. Si se excede el número máximo especificado por el fabricante, el rendimiento se deteriora rápidamente.

Dos puntos de acceso pueden comunicarse entre sí a través de la red cableada o mediante un enlace de radio entre ellos a modo de puente (*bridge* inalámbrico). En este último caso se suelen utilizar antenas direccionales, de mayor alcance, para intercambiar sus señales de radio.

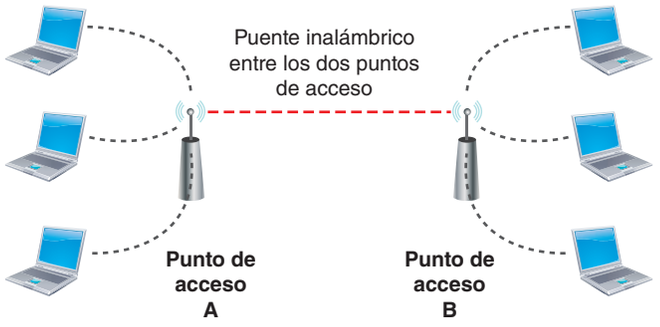


Fig. 7.15. *Enlace de dos puntos de acceso a través de un puente inalámbrico.*

En el nivel 2, Wi-Fi no es Ethernet. Además de otras diferencias operacionales se distingue fundamentalmente en que las tramas no son exactamente iguales y en que el protocolo de acceso al medio no es CSMA/CD como en Ethernet, sino CSMA/CA.

Por encima del nivel 2 (IEEE 802.11), las redes WLAN soportan los mismos protocolos que las redes cableadas, por eso una Wi-Fi puede transportar IP. Además, como las tramas Wi-Fi y las Ethernet, aunque distintas, son muy parecidas, resulta relativamente sencillo integrar la red cableada Ethernet con la red Wi-Fi inalámbrica, formando una red mixta.

Para que un cliente inalámbrico pueda transmitir al punto de acceso debe realizar antes dos operaciones:

- **Autorización.** El cliente presenta al punto de acceso la clave de acceso (si es un punto de acceso protegido) y el punto de acceso le validará.
- **Asociación.** Es la operación por la que un cliente inalámbrico establece un canal de comunicación con el punto de acceso una vez que este le ha autorizado a establecerlo.

Formalmente todas las estaciones asociadas a un punto de acceso identificado por su SSID forman con él lo que se llama una BSS *(Basic Service Set),* que es el equivalente a un segmento de red inalámbrico. Este BSS se identifica por un parámetro que es el BSSID *(BSS Identifier).*

Cuando las redes son grandes y es necesaria la instalación de más de un punto de acceso se pueden agrupar varios BSSID formando un ESSID *(Extended Service Set Identifier).* Todos los puntos de acceso que pertenecen al mismo ESSID deben tener el mismo identificador SSID. Esto permite que los clientes obtengan itinerancia sin perder el servicio a través de funciones de roaming.

Cuando una estación detecta la presencia de más de un punto de acceso elige el que le suministre mayor potencia de señal y la menor tasa de error, que suele ser el más cercano, aunque no necesariamente.

Si el cliente inalámbrico es móvil y se va desplazando a lo largo del rango del ESSID, puede que tenga que cambiar de punto de acceso sin cambiar de ESSID, lo que exige una **reasociación** con el nuevo punto de acceso. En esto consiste la itinerancia inalámbrica.

Los puntos de acceso pueden gestionar por sí mismos la reasociación de los clientes inalámbricos móviles o realizar esta función mediante un conmutador inalámbrico, que gestiona a todos los puntos de acceso y al que se conectan los puntos de acceso mediante red cableada.

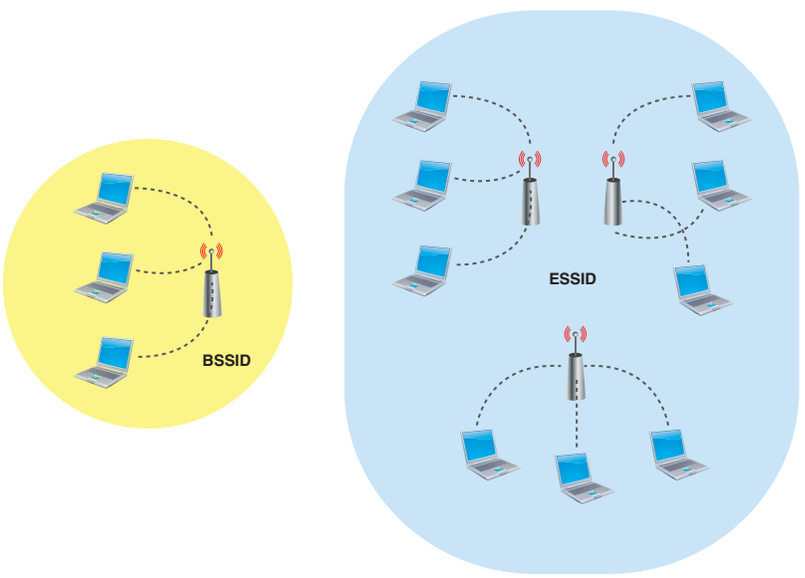


Fig. 7.16. *Representación de una BSSID (a la izquierda) y de una ESSID (a la derecha).*

CEO

SMR__RL_AAbad_07_IPv6.docx
Documento que contiene información sobre:
1. Formato de trama de IPv6.
2. Ámbitos de una red IPv6.
3. IPv6 sobre Windows y Linux.

2. Redes IPv6

La dificultad de conseguir direcciones públicas IPv4 ha hecho que los organismos internacionales de estándares se hayan propuesto renovar el protocolo IP para admitir un rango de direccionamiento mucho más extenso. IPv6 viene a corregir este problema, además de muchos otros relacionados con las mejoras en el encaminamiento de paquetes.

Aquí vamos a estudiar cómo son los paquetes IPv6 y su sistema de direccionamiento, intentando establecer analogías con el ya conocido IPv4.

En IPv6 se definen tres tipos de direcciones, todas de 128 bits de longitud:

- **Unicast:** son direcciones que se aplican a una única interfaz de red. Cuando un paquete es enviado a una dirección unicast, este se entrega a la única interfaz de red que posee esa dirección. Las direcciones unicast son, por tanto, únicas en la red.
- **Anycast:** es una dirección que identifica a un conjunto de interfaces, posiblemente a diferentes nodos. Un paquete enviado a una dirección anycast será entregado en una (y solo en una) de las interfaces que comparten la dirección anycast. Las direcciones anycast permiten crear ámbitos de redundancia. Por ejemplo, si en la instalación disponemos de dos enrutadores IPv6, podemos configurarlos con una única dirección anycast que los englobe a ambos y dirigir las peticiones de los clientes a esta única dirección compartida: alguno de los dos enrutadores atenderá la petición del cliente. Si uno de los enrutadores pierde su funcionalidad, el otro enrutador escuchará y atenderá todas las peticiones.
- **Multicast:** también es una dirección que identifica a un conjunto de interfaces, pero en este caso, cuando un paquete es enviado a una dirección multicast, el paquete será entregado en todas y cada una de las interfaces que posean esa dirección multicast y que estén operativas. Una dirección multicast es la apropiada para efectuar las retransmisiones de *broadcasting*.

Una interfaz debe tener al menos una dirección unicast única, pero además de esta dirección puede tener otras de tipo unicast, anycast o multicast.

2.1. Representación de direcciones IPv6

Una dirección IPv6 se puede escribir de modo genérico con una secuencia del tipo X:X:X:X:X:X:X:X, donde X representa un valor hexadecimal de 16 bits, que típicamente se numera con cuatro dígitos hexadecimales. Por ejemplo, una dirección IPv6 válida sería:

FF01:0000:0000:0A00:12DF:0000:0144:0001

Cada elemento de cuatro dígitos hexadecimales o 16 dígitos binarios se puede resumir. Por ejemplo, la dirección anterior se puede abreviar en la forma:

FF01:0:0:A00:12DF:0:144:1

Cuando varios grupos de dígitos contiguos están a cero, la cadena puede sustituirse por el símbolo «::». Este símbolo puede aparecer en cualquier lugar si fuera necesario, pero solo una vez. En nuestro ejemplo, se escribiría:

FF01::A00:12DF:0:144:1

Cuando nos encontramos en entornos en donde IPv6 debe convivir con IPv4 suele ser conveniente una notación mixta en donde los últimos 32 bits de la dirección IPv6 se escriben como si fueran una dirección IPv4. Por ejemplo, sería válida una dirección como:

::FFFF:192.168.150.23

Ampliación

IPv6 también puede expresar algo parecido a las subredes de IPv4 con una nomenclatura similar a la CIDR. Una dirección de «subred» IPv6 se denomina un prefijo de red y se expresa como una dirección IPv6 seguida de una barra «/» y de la longitud del prefijo en bits. Es muy común expresar la dirección IPv6 de una interfaz como el prefijo de la subred (por ejemplo, de n bits) más los 128-n bits de un identificador de interfaz, de modo que su dirección completa sea única.

En cuanto a las direcciones unicast, se han definido en el estándar IPv6 dos tipos: direcciones locales de enlace y direcciones locales de sitio. Las direcciones locales de enlace se utilizan en entornos en los que no hay enrutadores IPv6, que son los que proporcionan los parámetros de autoconfiguración en redes IPv6, de modo que suelen emplearse en situaciones en donde la autoconfiguración de cada nodo es importante, es decir, es el caso de las redes más básicas: algo equivalente a una red de área local aislada en IPv4. Estas direcciones tienen la siguiente estructura:

FE80::<ID de interfaz>/10

Donde <ID de interfaz> es la dirección MAC de la interfaz de red. En la anterior Fig. 7.13-D vimos que Linux nos había proporcionado una dirección IP automática de este estilo.

Las direcciones locales de sitio permiten direccionar dentro de un sitio local (típicamente un campus o un edificio) sin necesidad de un prefijo global. Estas direcciones se configuran mediante un identificador de subred, teniendo en cuenta que los encaminadores no deben enrutar fuera del sitio ningún paquete cuyo destino sea una dirección local de sitio, es decir, los enrutadores IPv6 no gestionan nunca tráfico local. La estructura de estas direcciones es:

FFC0::<ID de subred>:<ID de interfaz>/10

2.2. Direcciones reservadas

En IPv6 se han reservado algunos conjuntos de direcciones que permitan una transición cómoda entre IPv4 e IPv6. Por ejemplo, las direcciones que comienzan por «1111 1111» en binario, o FF en hexadecimal, corresponden a direcciones multicast.

Las direcciones anycast son tomadas del espacio propio de las direcciones unicast.

Hay algunas direcciones especiales en IPv6:

- **Dirección de *Loopback* o de retorno:** es la dirección «::1» (127 ceros seguidos de un 1 final). Se asigna a una interfaz virtual que hace de bucle interno en el nodo para identificar el arranque correcto de los protocolos. En IPv4, su dirección equivalente es la 127.0.0.1.
- **Dirección no especificada:** es la dirección «::», que no debe ser asignada nunca a ninguna interfaz puesto que representa la situación de la misma antes de que se le asigne cualquier otra dirección definitiva.
- **Dirección de túneles dinámicos IPv6 sobre IPv4:** son direcciones del tipo **«::<dirección IPv4>».** Se trata de 96 ceros seguidos por 32 bits que representan una dirección IPv4. Estos túneles se emplean para transmitir IPv6 a través de redes Ipv4 de modo transparente.
- **Direcciones IPv4 sobre IPv6:** son direcciones del tipo **«::FFFF:<dirección IPv4>»,** es decir, 80 bits a cero, seguidos de 16 bits a uno (FFFF en hexadecimal) y de 32 bits que representan una dirección IPv4. Estas direcciones permiten que los nodos que soportan IPv4 puedan seguir trabajando en redes IPv6.

2.3. Convivencia IPv4/IPv6

El encaminamiento de IPv6 es mucho más sencillo que el de IPv4 ya que en la definición original del protocolo se han tenido en cuenta las dificultades que presentaba IPv4 para ser enrutado.

IPv6 está pensado para que su enrutamiento sea semejante al de IPv4 con CIDR, sin embargo, se han mejorado sustancialmente los problemas que presenta IPv4 cuando se cambia de proveedor: el nuevo proveedor de Internet no podrá respetar las direcciones IP fijas que asignó el antiguo proveedor a los servidores Internet de la instalación que contrató sus servicios.

Ampliación

Una primera aproximación para hacer convivir IPv4 e IPv6 consiste en que los nodos tengan dos pilas de protocolos: una IPv4 y otra IPv6. Cada comunicación utilizará la pila de protocolos que requiera el servicio que deba proporcionar.

Una segunda posibilidad es conseguir tunelizar IPv6 dentro de túneles IPv4, de este modo los paquetes IPv6 podrán viajar a través de la Internet tradicional, que de momento utiliza mayoritariamente IPv4. En el otro extremo del túnel, los enrutadores extraerán los paquetes IPv6 del túnel y los entregarán a sus destinatarios IPv6. Se exige, por tanto, que los encaminadores que están en la frontera de la instalación e Internet gestionen ambas pilas de protocolos.

Una vez que Internet vaya pasando a IPv6, el problema será justo el contrario: habrá nodos IPv4 en las instalaciones de los usuarios que requerirán comunicarse mediante redes IPv6. La solución a este problema será semejante: se crearán túneles IPv6 en los que se tunelizarán comunicaciones IPv4.

Para facilitar estas transiciones, la mayor parte de los sistemas operativos modernos incorporan de modo nativo las dos pilas de protocolos, aunque se deja libertad a los administradores de sistemas para que sean o no configurados.

	Lanzado en	Tamaño de las direcciones	Formato de las direcciones	Notación de prefijos	Cantidad de direcciones
Protocolo de Internet versión 4 (IPv4)	1981	Número de 32 bits	Notación decimal con puntos: 192.149.252.76	192.149.0.0/24	2^{32} = ~ 4,000,000,000
Protocolo de Internet versión 6 (IPv6)	1999	Número de 128 bits	Notación hexadecimal: 3FFE:F200:0234:AB00:0 123:4567:8901:ABCD	3FFE:F200:0234::/48	2^{128} = ~ 340,000,000, 000,000,000,000,000, 000,000,000,000,000

Tabla 7.3. *Características comparativas de IPv4 e IPv6.*

Esto implicará que los encaminadores en Internet tendrán que sustituir sus tablas de rutas para que los servidores sean alcanzables con las nuevas direcciones que el proveedor nuevo haya asignado a estos servidores. Además, en la instalación deberán sustituirse las antiguas direcciones IPv4 por las nuevas, así como los registros de los servidores DNS en donde fueron declaradas.

Con la tecnología IPv6 esto no es necesario. Cada interfaz IPv6 tendrá una dirección compuesta por un elemento local, generalmente ligado a la interfaz o asignado por el administrador de red y que es único en su instalación, precedido por un prefijo de red global que es asignado por el router de la instalación automáticamente a cada nodo. Este prefijo, o al menos parte de él, es a su vez asignado por las autoridades de asignación de números en Internet, por ejemplo la IANA.

Ampliación

Cuando una instalación cambia de proveedor, no será necesario que cambie sus direcciones locales, basta con que cambie su prefijo de enrutamiento, lo que se hace en el encaminador y no en cada nodo. Por tanto, las transiciones de cambio de proveedor serán mucho más sencillas, ya que la dirección IPv6 es articulada.

Por otro lado, la mayor parte de los nodos en Internet y en las instalaciones de los usuarios son IPv4. La transición a IPv6 no se puede hacer de golpe sino que exige un cuidadoso estudio para que durante un tiempo convivan las dos tecnologías simultáneamente.

Investigación

En la página **http://www.taringa.net/posts/apuntes-y-monografias/1392609/que-es_-y-como-va-ser-la-ipv6_.html** tienes mucha información sobre IPv4 e IPv6. Fíjate especialmente en la imagen de esa página accesible desde **http://www.millenniasystems.com/downloadables/IPv6%20Protocol%20Comparison%20to%20IPv4.jpg** para estudiar las analogías y diferencias de los protocolos IPv4 e IPv6.

Actividades

6. Relaciona los elementos de la columna de la izquierda con los de la derecha:

Dirección	Significado
FE80::	Túnel IPv6 sobre IPv4
FFC0::	Dirección no especificada
::	Dirección de *loopback*
::1	Direcciones locales de sitio
::192.168.10.20	Direcciones locales de enlace
::FFFF:192.168.10.20	Direcciones IPv4 sobre IPv6

7. Escribe en la forma IPv6 más abreviada posible las siguientes direcciones IPv6 e IPv4:

Dirección IPv6 o IPv4	Forma abreviada IPv6
FF01:0000:0000:0000:0000:0000:0144:0001	
FF01:0000:0000:0000:12DF:0000:0144:0001	
0000::1	
192.168.20.20	
0000::FFFF:192.168.10.20	

8. Para realizar este ejercicio necesitarás dos PC clientes (uno con Windows Vista y otro con una distribución Linux con IPv6 nativo). Después realiza las siguientes operaciones.

a) Configura el cliente Windows con una dirección IPv6 del tipo ::<IPv4>.

b) Haz lo mismo con el cliente Linux, pero asígnale su propia dirección IPv6.

c) Comprueba que puedes hacer ping entre ambas estaciones utilizando IPv6.

Ayuda: para hacer ping utilizando IPv6 necesitarás una utilidad ping especial *ping ipv6…* en Linux y *ping6* en Windows.

3. Redes privadas virtuales

Una red privada virtual o **VPN** *(Virtual Private Network)* es una red que soporta transporte de datos privados sobre infraestructura pública utilizando los mismos mecanismos de seguridad, gestión y políticas de acceso de una LAN. Normalmente la red pública de transporte es de tipo IP, habitualmente Internet. Muchos routers y *firewalls* son capaces de crear y aceptar conexiones VPN. La funcionalidad VPN se puede obtener con hardware especializado o mediante software. Por ejemplo, OpenVPN es un software de creación de VPN con licencia GPL sobre muchos sistemas operativos.

Podríamos clasificar inicialmente las VPN en tres tipos diferenciados dependiendo del tipo de servicio que proveen.

- **VPN de acceso remoto.** Conectan teletrabajadores y, en general, usuarios móviles.
- **VPN de Intranet.** Conecta ubicaciones fijas o delegaciones de oficinas dentro de una WAN corporativa utilizando conexiones dedicadas.
- **VPN de Extranet.** Proporciona acceso limitado a los recursos informáticos internos de las empresas a sus colaboradores, proveedores, clientes, etc. Es el fundamento tecnológico de algunos portales verticales en Internet dedicados al comercio electrónico.

Ampliación

Las VPN utilizan protocolos de seguridad como IPSec o L2TP, que estudiaremos seguidamente. Por otra parte, los sistemas operativos actuales incorporan el software VPN en sus configuraciones básicas. Por ejemplo, Windows tiene todos los elementos necesarios para desplegar rápidamente una VPN que solucione problemas en muchos escenarios diferentes. Linux también se utiliza frecuentemente como plataforma base para la construcción de VPN.

3.1. Protocolo SSL

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

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

- En la primera fase el navegador solicita una página a un servidor seguro. La petición queda identificada por el protocolo https en vez de http, utilizado en páginas no seguras. A continuación, navegador y servidor negocian las capacidades de seguridad que utilizarán a partir de ese momento.
- Seguidamente, se ponen de acuerdo en los algoritmos que garanticen la confidencialidad, integridad y autenticidad.
- En una tercera fase, el servidor envía al navegador su certificado de norma X.509, que contiene su clave pública y, si la aplicación lo requiere, solicita a su vez el certificado del cliente. Con esta operación quedan identificados y autenticados.
- A continuación, el navegador envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos que se hayan de intercambiar como seguros. El envío de esta clave se hace cifrándola con la clave pública del servidor que extrajo previamente de su certificado.
- Finalmente, se comprueba la autenticidad de las partes implicadas y, si el canal ha sido establecido con seguridad, comenzarán las transferencias de datos.

Ampliación

Aunque las claves generadas por SSL son débiles, es difícil romperlas en el tiempo que dura una transacción, por lo que, sin ser el mejor protocolo de seguridad, es suficientemente válido. SSL es uno de los protocolos más utilizados en la creación de redes privadas virtuales. SSL, sin embargo, no resuelve el problema de la autenticación.

Ampliación

Los certificados X.509 están contenidos en ficheros que pueden tener las siguientes extensiones:

- **CER** o **DER:** certificados codificados como CER o DER.
- **PEM:** certificado codificado en Base64.
- **P7B** o **.P7C:** estructura de datos en formato PKCS#7.
- **PFX** o **.P12:** pueden contener certificados o claves privadas.

Para obtener más información, puedes consultar **http://es.wikipedia.org/wiki/x.509.**

Ampliación

Los **certificados X.509** se utilizan para garantizar que una clave pública pertenece realmente a quien se atribuye. Son documentos firmados digitalmente por una autoridad de certificación, que asegura que los datos son ciertos tras demostrárselo el solicitante del certificado documentalmente. Contienen la clave pública, los datos que identifican al propietario, los datos de la autoridad de certificación y la firma digital generada al encriptar con la clave privada de la autoridad de certificación.

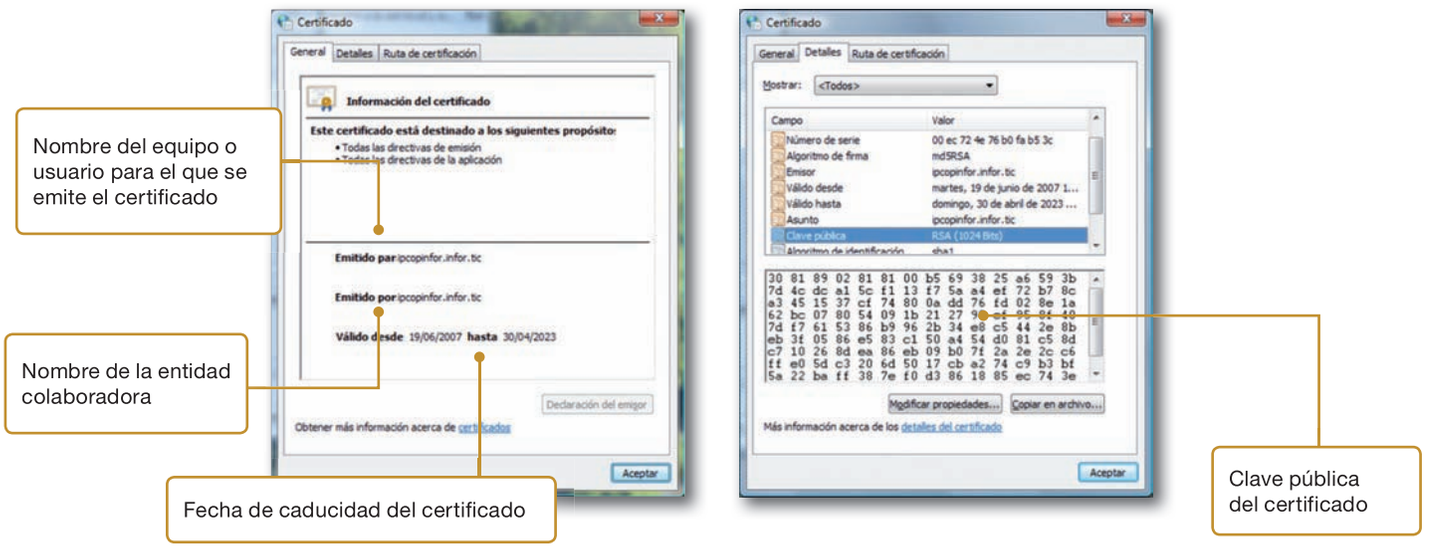


Fig. 7.17. *Ventanas informativas de un certificado exportado en la norma X.509.*

SSL aporta muchas ventajas a las comunicaciones seguras. En primer lugar, goza de gran popularidad y se encuentra ampliamente extendido en Internet. Está soportado por todos los navegadores actuales. Además asegura cualquier comunicación punto a punto, no necesariamente de transmisión de páginas web, aunque esta es la aplicación de mayor uso. Por último, el usuario no necesita realizar ninguna operación especial para activar el protocolo: basta con sustituir en el navegador la secuencia http por https en el URL.

CEO

SMR_RL_AAbad_07_SET.docx

Documento que contiene información sobre protocolo SET para comercio electrónico.

3.2. Protocolo SSH

En el mundo de los sistemas operativos ssh es el nombre de una utilidad que sirve para acceder a máquinas remotas a través de la red. Es semejante a telnet pero, a diferencia de telnet, que no cifra la conexión, ssh sí que la encripta, lo que hace que las conexiones sean mucho más seguras.

Sin embargo, en el universo de las redes, **SSH** (*Secure Shell,* intérprete de órdenes seguro) es el nombre del protocolo utilizado para realizar estas conexiones cifradas.

SSH puede manejar sesiones tanto de consola textual como gráficas. Sobre SSH se implementan muchas aplicaciones (ssh es una de ellas) que permiten realizar múltiples operaciones como copiado de ficheros, realización de backups, etc., realizando túneles punto a punto entre los dos extremos de la comunicación. Así surgen nuevos protocolos basados en SSH como **SCP** *(Secure Copy)* o **SFTP** *(Secure File Transfer Protocol).*

La implementación de ssh se lleva a cabo como un cliente en un extremo y un servidor ssh en el otro. Entre ellos se establecen los túneles por los que viajan los datos cifrados. La seguridad de SSH se basa en el cifrado de clave pública.

El desarrollo de software libre más extendido para un servidor SSH es OpenSSH. En la versión cliente suele ser muy utilizado PuTTY. Otras aplicaciones libres que pueden utilizarse para la transmisión de ficheros son WinSCP o Filezilla.

3.3. Tecnologías relacionadas con IPSec

Cuando hablamos de **IPSec** nos referimos a un conjunto de extensiones del TCP/IP que añaden autenticación y encriptación en la transmisión de paquetes. IPSec genera paquetes de datos que constan de tres elementos diferenciados: cabeceras de autenticación, bloques de seguridad y un protocolo de negociación e intercambio de claves.

A. Protocolo L2TP

L2TP *(Layer Two Tunneling Protocol)* es una extensión del protocolo PPP que permite la operación con redes privadas virtuales tomando lo mejor de los protocolos PPTP (*Point to Point Tunneling Protocol*, su protocolo homólogo de Microsoft) y L2F de Cisco Systems. Para que una conexión L2TP tenga lugar, es necesario que los enrutadores por los que pase la conexión sean compatibles con L2TP. Ambos protocolos toman como base PPP.

L2TP es una tecnología de redes compatible con las redes privadas virtuales multiprotocolo que permite a los usuarios tener acceso seguro a redes empresariales a través de Internet. La ventaja de L2TP sobre PPTP reside en que L2TP no depende de las tecnologías específicas del fabricante.

B. El protocolo IPSec

IPSec es un marco de trabajo para todo un nuevo grupo de especificaciones orientadas a conseguir comunicaciones seguras. Cuando dos estaciones quieren comunicarse a través de IPSec, establecen una asociación de seguridad o SA intercambiando sus claves de seguridad. En la SA se mantiene la información del protocolo IPSec empleado (AH o ESP), los algoritmos de encriptación y autenticación, las claves utilizadas y el tiempo de vida de las mismas. A partir de ese momento, las comunicaciones serán totalmente seguras.

En la configuración de IPSec de un equipo se puede elegir que todas las comunicaciones sean seguras y se descarten todas las peticiones que no sean seguras o bien que aunque se habilite la seguridad, se atiendan las peticiones inseguras. En este último caso, el cliente es quien decide si utilizará un transporte seguro o no, ya que el servidor atendería tanto las peticiones seguras como las inseguras.

La configuración de IPSec sobre Windows se puede hacer con las consolas gráficas de gestión de directivas. En Linux se utiliza la línea de comandos.

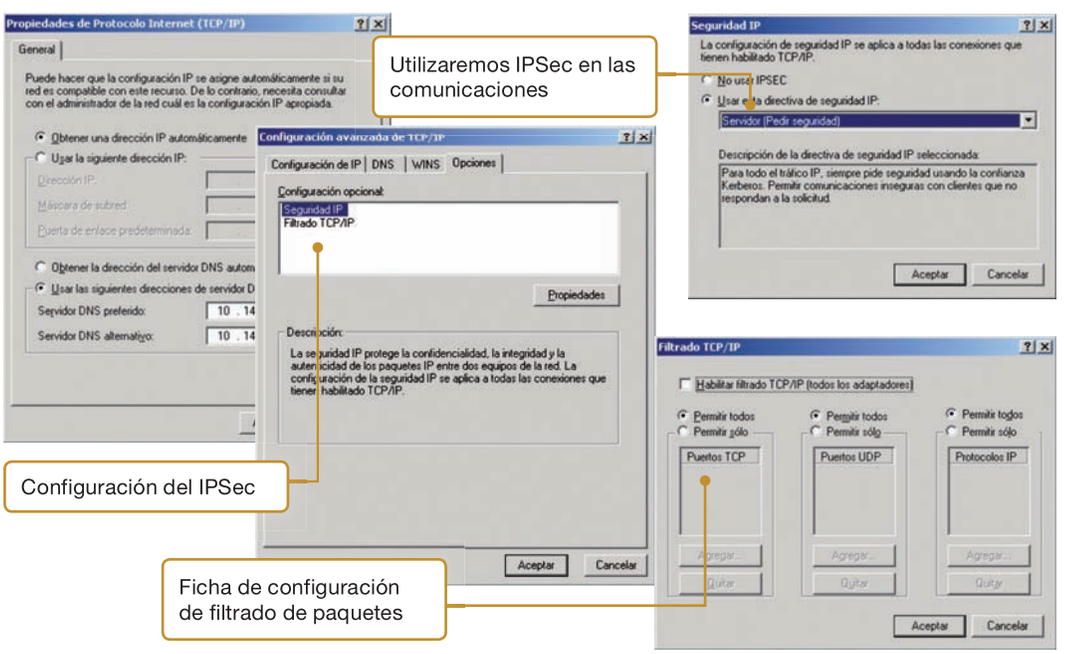


Fig. 7.18. *Fichas de configuración de IPSec y de filtrado de paquetes en Windows.*

Actividades

9. Busca los errores en el siguiente razonamiento:

«Los clientes de mi oficina acceden a las aplicaciones web corporativas mediante el protocolo http desde su navegador de Internet. Para que las aplicaciones http sean seguras se ha habilitado SSL. El servidor utiliza tantos certificados X.509 como usuarios acceden a sus aplicaciones: cada uno utiliza el suyo y así quedan todos identificados».

10. Relaciona en la siguiente tabla las tecnologías de la columna de la izquierda con los elementos de la columna de la derecha:

Tecnología	Significado
X.509	Encriptación de la información
SSL	Transporte seguro
IPSec	Certificado digital
VPN	Acceso remoto mediante túneles
https	Acceso web mediante SSL

11. Describe cuáles son los escenarios típicos en que se puede utilizar la tecnología de redes IPsec.

Ampliación

En las redes mixtas entre redes de cable e inalámbricas el punto tecnológico crítico son los puntos de acceso y su integración en las redes cableadas. Si el punto de acceso deja de funcionar tendremos un conjunto de clientes inalámbricos sin posibilidad de acceso a los recursos de la red. Esta es la razón por la que se aconsejan que, en este tipo de redes mixtas, los puntos de accesos estén duplicados.

4. Modelos de integración de redes

Salvo que la red sea muy pequeña, lo normal es que toda red presente una gran diversidad de tecnologías de diferentes naturalezas. No todas las tecnologías cubren todas las necesidades del administrador de red en su afán de proporcionar los servicios que se le solicitan. Otras veces la diversidad se produce por el propio crecimiento paulatino de la red, por ejemplo, en un principio se construyó una red cableada, pero la introducción de portátiles con tecnología inalámbrica hace que esta red cableada deba ser extendida con una WLAN. Vamos a estudiar aquí cuáles son los factores que intervienen en el polimorfismo de las redes y que hacen que toda red de un cierto volumen sea una red tecnológicamente mixta.

4.1. Atendiendo al sistema de cableado

La red cableada es la columna vertebral de cualquier red de área local. Tecnológicamente interesa que el cableado esté desplegado según las normas de cableado estructurado. Lo normal es que todos los servidores tengan al menos una conexión a la red de cableado y, si tuvieran que soportar un volumen de tráfico considerable, interesa que la línea de conexión sea de alta velocidad.

Por otra parte, los clientes pueden conectarse a los servicios a través de la propia red de cableado estructurado o mediante conexiones inalámbricas. Si se hace un despliegue inalámbrico hay que prever que el ancho de banda de un punto de acceso inalámbrico es menor que el de un acceso cableado Ethernet y que además está compartido entre todos los clientes. Si algún cliente va a generar mucho tráfico hay que reconsiderar si fue una buena decisión que su acceso fuera inalámbrico porque no solo experimentará un cuello de botella en sus comunicaciones sino que también perjudicará a las de sus clientes inalámbricos vecinos.

4.2. Atendiendo al sistema de direccionamiento de la red y a la arquitectura de protocolos

Aunque en la actualidad se tiende a que todos los sistemas operativos de red «hablen» TCP/IP, es posible que haya alguna máquina en la red que no cumpla este requisito o que, cumpliéndolo, suministre algún servicio utilizando protocolos de alguna otra arquitectura. En este caso, la integración del equipo en la red deberá estudiarse con arreglo a la documentación que suministre el fabricante. Aun así, no en todos los casos será posible realizar totalmente esta integración. En muchos casos será necesaria la asistencia de dispositivos de red muy complejos (pasarelas) que hagan la traducción entre los protocolos utilizados por los clientes y por los servidores.

Ampliación

Otro ámbito de integración es el sistema de direccionamiento aun dentro de la misma familia. Por ejemplo, es posible que en una misma red TCP/IP convivan nodos con IPv4 y otros con IPv6. En este caso, el protocolo IPv6 tiene en cuenta este problema y proporciona las herramientas necesarias para integrar todos los equipos sin demasiada dificultad, utilizando sistemas de direccionamiento en los que parte de la dirección IPv6 es justamente la dirección IPv4 y haciendo convivir ambas pilas de protocolos simultáneamente sobre la misma interfaz de red.

4.3. Atendiendo a los sistemas operativos de red

De modo análogo a las redes, algo parecido ocurre con los sistemas operativos de red. Cada equipo que se conecta a la red tiene su propio sistema operativo. El administrador de red tiene alguna capacidad de decisión sobre ellos, pero tampoco demasiada. Por tanto, cuando diseña los servicios de la red tiene que tener en cuenta que la tecnología de software que posee hoy, seguro que habrá evolucionado mañana. Esto le obliga a someterse al imperio de los estándares. Afortunadamente, los fabricantes de software se pliegan a estos estándares facilitando la labor del administrador de red.

En principio, cuando se tiene que proveer un servicio en la red se ha de procurar que ese servicio será accedido por clientes con diferentes sistemas operativos, no solo en cuanto al fabricante, sino en cuanto a las versiones. Las pruebas de servicio deben hacerse en laboratorio y, solo cuando se hayan comprobado las prestaciones desde diferentes clientes, se abrirá el servicio a la producción.

Cuando las tecnologías son dispares, a veces el administrador tiene que imponer algunas restricciones a los clientes. Por ejemplo, alguna impresora moderna tiene un controlador para Windows, pero no lo tiene aún para Linux y, por tanto, solo podrá ser accedida por clientes Windows.

4.4. Atendiendo al modo de acceso de los clientes

Cada servicio tiene una identidad propia en la red: discos, impresoras, aplicaciones, etc. Para acceder a un servicio no solo hace falta conocer su identidad (tipo de servicio, cómo se llama, para qué sirve) sino que hay que conocer cómo se accede a él. La respuesta a esta cuestión depende del servicio concreto, pero también de quién sea el cliente y de dónde esté situado en la red. No es lo mismo un cliente que accede por módem que otro que accede directamente al servicio porque está situado en la propia LAN.

Según este modelo de acceso de clientes podemos distinguir las siguientes posibilidades:

- **Acceso local conmutado.** Los clientes están en la misma red local que el servidor y acceden directamente. El acceso al servicio puede requerir autenticación si el protocolo servidor lo admite, pero la red local no pondrá ningún obstáculo. La conexión entre el cliente y el servidor se realiza a través de un sencillo conmutador.
- **Acceso local autenticado.** Clientes y servidor están también en la misma LAN, pero el acceso al servidor requiere autenticación. Este es el caso de utilización de IPSec dentro de la misma LAN o el caso de PPPoE (un modo de utilizar Ethernet con autenticación). Solo las conexiones autenticadas competirán por los recursos del servidor. Aparte de esta autenticación, puede que el servicio (dentro del servidor) requiera una nueva autenticación. Por ejemplo, para acceder al servidor se requiere un certificado digital concreto.

  Una vez ganado el servidor, para acceder a cierta carpeta compartida de ese servidor, hay que proporcionar un nombre de usuario y contraseña.
- **Acceso remoto autenticado.** El cliente se halla en una localización remota al servidor. Su acceso puede ser mediante módem o a través de Internet, y normalmente utiliza algún método de autenticación para preservar el acceso. Este sería el caso de utilización de RAS con protocolo PPP para ganar la red local desde el exterior.
- **Acceso por VPN.** El cliente remoto utiliza una red pública para crear un túnel seguro que le permita ganar el acceso a la red local. Los datos viajarán encriptados por el túnel, pero la tecnología utilizada tanto en el cliente como en el servidor serán propias de la LAN. En la creación del túnel se puede requerir la autenticación del cliente.

CEO

SMR_RL_AAbad_07_VPN-EnrutamientoWindows.pptx

Documento que contiene realizaciones prácticas sobre:

1. Creación de un escenario para la creación de rutas dinámicas.
2. Instalación y configuración de Microsoft IAS.
3. Gestión del enrutador sobre Windows Server.
4. Creación y gestión de NAT.
5. Instalación de un doble enrutador IAS.
6. Utilización de los protocolos de enrutamiento RIPv2 y OSPF.
7. Instalación y configuración de un servidor VPN con IAS.
8. Creación de conexiones de cliente VPN.
9. Monitorización de las conexiones.

Claves y consejos

Hay que tener en cuenta que en la actualidad cobran mucha importancia los accesos de la red desde dispositivos inalámbricos que tienen sus propios sistemas operativos y que habrá que integrar con la red corporativa, tanto desde dentro como desde fuera de la empresa.

Ampliación

Escenarios típicos para la utilización de IPSec

Los escenarios más comunes en que se suele implantar IPSec son cuatro. La elección de uno u otro dependerá de las características de la red. No hay que olvidar que IPSec se instala encima de una red IP ya establecida y de las necesidades de comunicación corporativas.

De router a router: en este caso, IPSec se ejecuta en un router situado en un sitio corporativo y en otro router en un sitio remoto. La encriptación se realizará entre los dos dispositivos, pero se deja sin encriptar el enlace entre el router y la estación final.

De cliente VPN a router o cortafuegos: proporciona conectividad segura para usuarios de estaciones móviles corporativas.

De cortafuegos a cortafuegos o de cortafuegos a router: funciona a modo de pasarela de red.

De router a múltiples routers o de router a múltiples cortafuegos: es una configuración muy común para corporaciones multinacionales que disponen de redes VPN.

Ampliación

Las tecnologías que separan de algún modo la tecnología del cliente de la del servidor son las que están más pujantes en la actualidad, precisamente para salvar el problema de la diversidad de sistemas operativos, tanto en servidor como en cliente. Entre otras, esta es una razón por la que proliferan las aplicaciones web que solo requieren un explorador con independencia del sistema operativo sobre el que están instalados o tecnologías como Java o lenguajes de script que son interpretados, obviando la instalación concreta tanto de software como de hardware.

Caso práctico 2

Configuración de un router inalámbrico

Imaginemos que una compañía tiene varias sedes repartidas por distintos lugares geográficos lejanos. Cada sede periférica se conecta a una sede central mediante Internet.

Tradicionalmente, como el volumen de tráfico que tenían que transmitir ha sido pequeño, se hacían conexiones esporádicas por módem para efectuar las transmisiones. Desde hace algún tiempo, el volumen de datos que hay que transmitir ha crecido significativamente y ha subido espectacularmente la factura telefónica.

El administrador de red ha determinado que es más barato contratar un acceso ADSL en cada oficina y ha solicitado al proveedor un encaminador inalámbrico para no solo tener un acceso de alta velocidad a Internet sino proveer a los clientes de conexiones inalámbricas. El proveedor le ha enviado una caja que contiene el router inalámbrico y una carta en la que le informa de que ya tiene servicio de conexión a Internet y los parámetros de conexión. Seguidamente extrae el encaminador de la caja, lo conecta a la línea de teléfono por la que le suministran ADSL y procede a la configuración del enrutador.

Vamos a exponer la configuración de un encaminador que incorpora además un punto de acceso inalámbrico y que por tanto construirá una red mixta.

Esto quiere decir que el enrutador dispondrá de dos interfaces: LAN y WAN, pero también que, además, la LAN podrá incorporar nodos inalámbricos Wi-Fi.

Normalmente estos routers se configuran vía web. Para ello, solo hay que conocer la dirección IP que el fabricante instala en sus dispositivos. Después de la primera conexión podremos cambiar esta dirección IP para adecuarla a las necesidades de nuestra red. En nuestro caso, la página web del router es accesible por el puerto 8080 de la dirección 192.168.10.253.

En la Fig. 7.19 vemos cómo podemos configurar los parámetros de la red inalámbrica que constituye la LAN. En ella configuramos el SSID, que en nuestro caso es «default», y el canal que utilizaremos en las comunicaciones, que será el 6. Los parámetros que nos quedan por configurar serán la autenticación y la encriptación. Nosotros hemos elegido una autenticación de sistema abierto y una encriptación WEP de 64 bits cuya clave es «aetae».

Una vez que hemos pasado por este punto ya tenemos lista nuestra red local inalámbrica para admitir conexiones de clientes inalámbricos.

Seguidamente tendremos que configurar la interfaz WAN del encaminador (Fig. 7.20), que en este router es una puerta Ethernet. Tendremos que configurar la dirección IP de la interfaz WAN: nosotros hemos elegido una dirección IP estática (192.168.10.253), con una máscara de red (255.255.255.0), una puerta de enlace (192.168.10.251) y

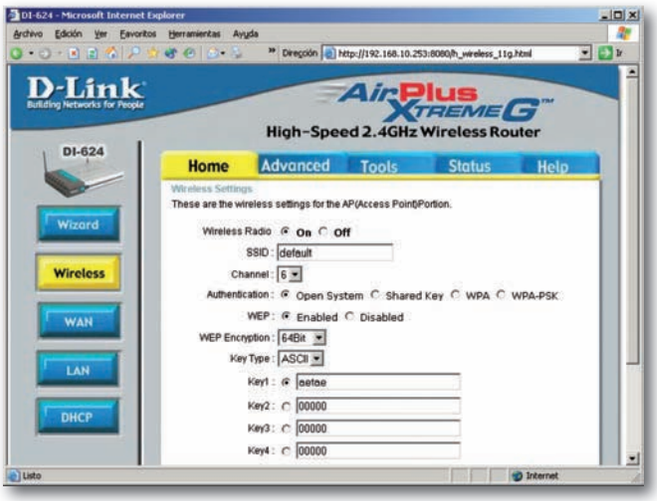


Fig. 7.19. *Configuración de la red inalámbrica.*

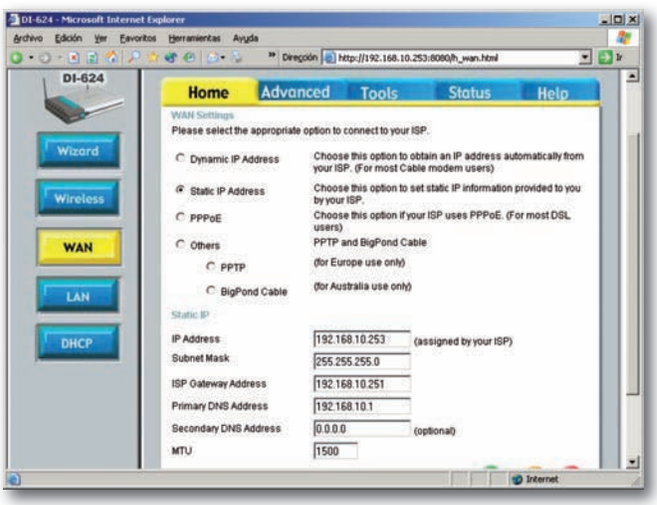


Fig. 7.20. *Configuración del segmento WAN del encaminador.*

un DNS que apunta a 192.168.10.1. Estos serían los datos que nos proporcionaría el proveedor de Internet.

Podemos observar que el router nos permite realizar conexiones a Internet utilizando un DHCP del proveedor *(Dynamic IP Address),* una IP estática (que es nuestro caso), utilizar PPPoE (una conexión Ethernet con autenticación semejante al acceso con módem, pero con la velocidad de Ethernet) u otros sistemas como PPTP.

A partir de aquí, ya hemos enseñado al router a salir a Internet.

La interfaz LAN de este router se compone de cuatro puertas Ethernet al que se añade la interfaz inalámbrica, que también es LAN. ¿Cómo puede conocer el encaminador qué es LAN y qué es WAN? La respuesta es: definiendo las direcciones IP y la máscara de la red LAN. Hay que tener en cuenta que las estaciones inalámbricas tienen

Continúa...

Caso práctico 2

...Continuación

que participar de este conjunto de direcciones IP, de lo contrario no se podrán comunicar con el router. Nosotros elegiremos la dirección 192.168.100.254 con máscara 255.255.255.0 (Fig. 7.21). Debemos observar que la dirección de red del segmento LAN (192.168.100/24) es incompatible con la dirección de red del segmento WAN que era 192.168.10.0/24. Por tanto, quedan perfectamente separados los nodos de la LAN de los de la WAN. Precisamente el router será el dispositivo encargado de su interconexión.

El encaminador posee un servidor DHCP por si deseamos utilizarlo (Fig. 7.22). Este servidor, una vez activo, se encargará de asignar direcciones IP a los clientes del segmento LAN. Debe observarse que el rango de direcciones IP que tendría que servir a la LAN debe estar comprendido dentro del ámbito de direcciones IP definidos para la LAN. El servidor DHCP también puede asignar direcciones IP concretas a clientes con direcciones MAC específicas, aunque en nuestro caso no hemos hecho ninguna asignación. Hemos elegido el ámbito de direcciones comprendidas entre la 192.168.100.100 y la 192.168.100.192. La dirección IP se concederá al cliente DHCP por una semana.

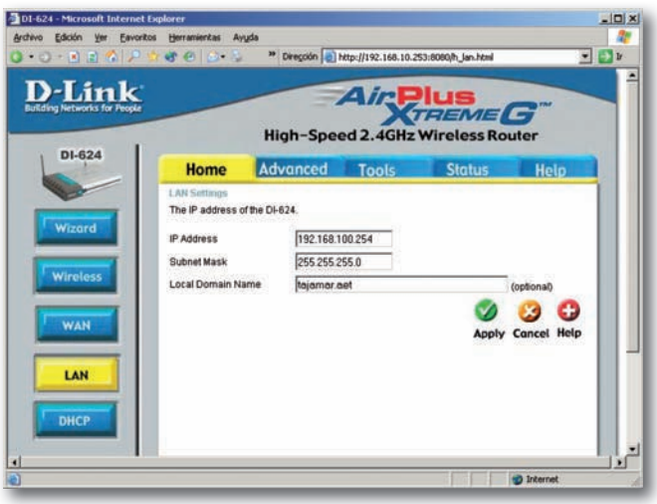


Fig. 7.21. *Configuración del segmento LAN del encaminador inalámbrico.*

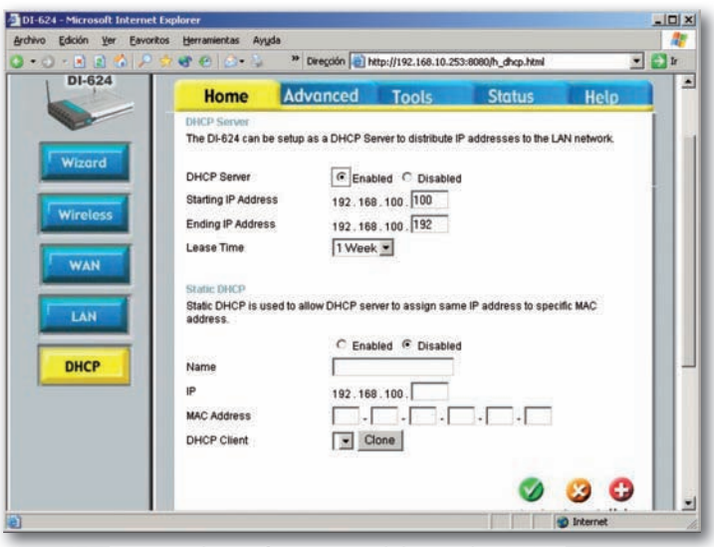


Fig. 7.22. *Página de configuración del servidor DHCP del encaminador.*

Claves y consejos

Antes de instalar un servidor DHCP en una red, hay que probar con antelación que no existe otro DHCP en la misma red. Puede hacerse conectando una estación configurada para obtener su dirección IP automáticamente. Si en la red ya hay otro DHCP, este nos servirá la dirección.

Si un mismo segmento de red tiene más de un servidor DHCP, no sabremos qué servidor DHCP nos brindará su servicio y se podrán producir colisiones de direcciones IP asignadas.

Además de un punto de acceso, el encaminador que estamos configurando tiene capacidades de *firewall*. Esta es la razón por la que podremos configurar la publicación de servidores desde la LAN a la interfaz WAN (Fig. 7.23) y las reglas de filtrado.

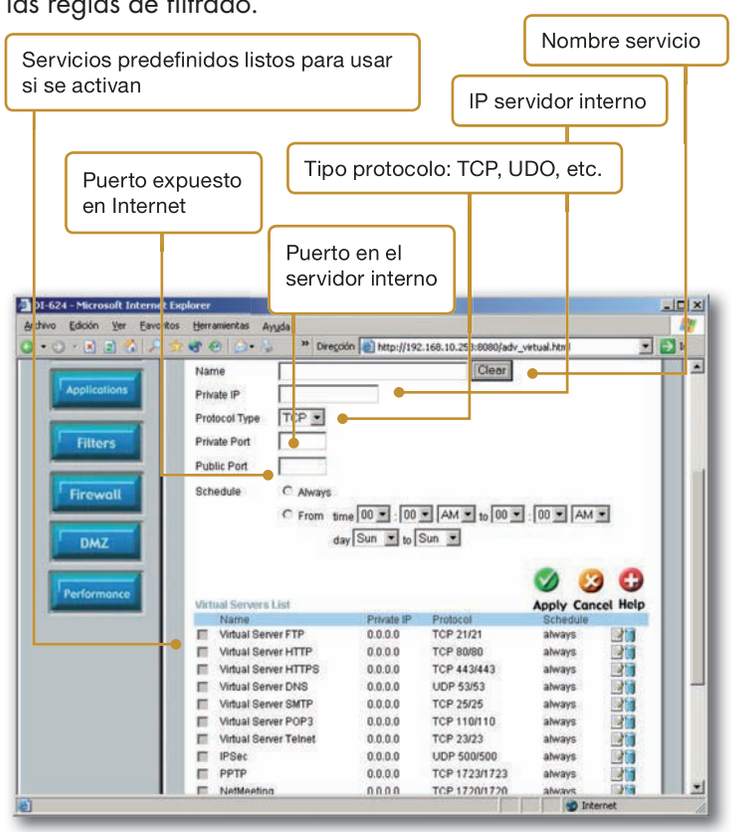


Fig. 7.23. *Publicación de servidores en el cortafuegos del encaminador inalámbrico.*

Continúa...

Caso práctico 2

...Continuación

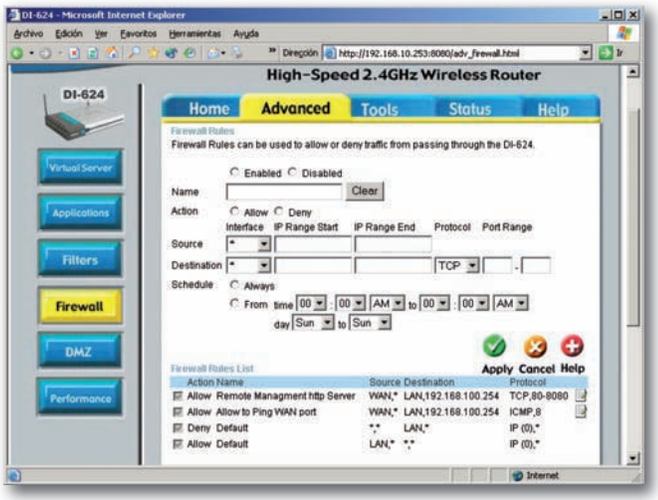


Fig. 7.24. *Declaración de los filtros en el cortafuegos.*

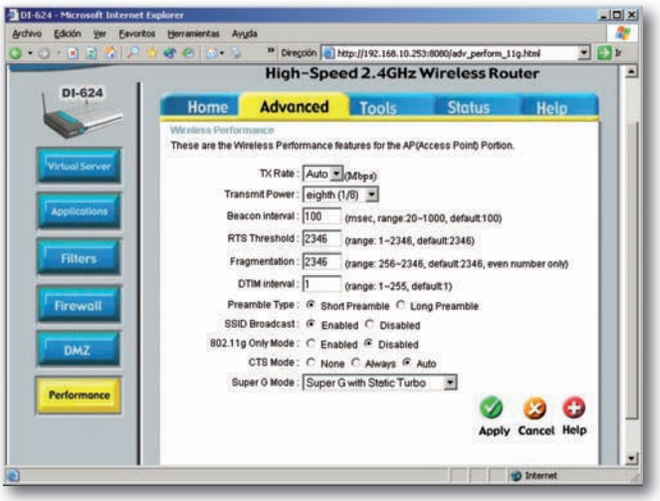


Fig. 7.26. *Configuración avanzada de Wi-Fi.*

Podemos ver que se pueden definir reglas de filtrado (Fig. 7.24) desde una red origen a una red destino, por rangos de direcciones IP. También podemos seleccionar el tipo de protocolo de comunicación al que le aplicaremos el filtro y el rango de puertos filtrados para ese protocolo. También se puede definir un sencillo calendario en que se aplicaría el filtro. Además, cada filtro puede tomar dos acciones: paquete permitido *(Allow)* o paquete denegado *(Deny)*.

La red DMZ permitida por este encaminador es muy pobre, ya que se compone exclusivamente de un solo nodo. En la página de configuración de la DMZ (Fig. 7.25) informaremos al router de la dirección IP del nodo que compondrá nuestra DMZ, que, en nuestro caso, será 192.168.100.51. Debemos observar que, en este modelo de DMZ, la dirección IP del nodo que la compone debe estar en el ámbito de la LAN, lo que confirma la pobreza de la red perimetral que puede construir en encaminador.

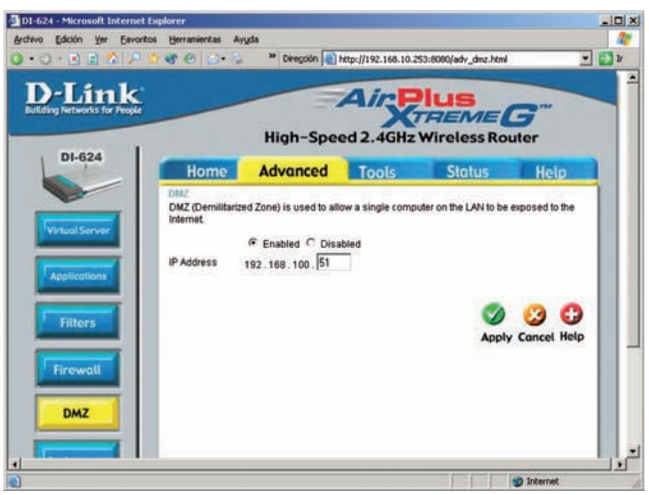


Fig. 7.25. *Configuración de la DMZ.*

En la página de prestaciones *(Performance)* podremos configurar las opciones avanzadas de la tecnología inalámbrica (Fig. 7.26). En esta página configuramos el punto de acceso para decirle que ajuste automáticamente la velocidad de transmisión entre el punto de acceso y las estaciones inalámbricas, que queremos solo 1/8 de la potencia máxima en la antena del punto de acceso, así como otros parámetros avanzados. Nos fijaremos especialmente en que tenemos habilitado el parámetro «SSID Broadcast». Esto quiere decir que el punto de acceso irá enviando tramas por las que informará a las estaciones inalámbricas de su existencia, es decir, que las estaciones descubrirán al punto de acceso automáticamente.

Como hemos deshabilitado el parámetro «802.11g Only Mode», el punto de acceso integrado al encaminador admitirá clientes 802.11b y 802.11g.

El resto de los parámetros se han elegido tomando los defectos de fábrica y no son especialmente significativos para nuestro propósito.

Hemos de fijarnos en el último parámetro «Super G Mode». Se trata de un modo de radiación específico del fabricante del encaminador, fuera de estándar, que acelera las comunicaciones. Si los clientes inalámbricos también fueran del mismo fabricante, quizá podríamos habilitarlo, pero si los clientes son de diversos fabricantes, tendremos que deshabilitar necesariamente este parámetro para ajustarnos al estándar.

Continúa...

Caso práctico 2

...Continuación

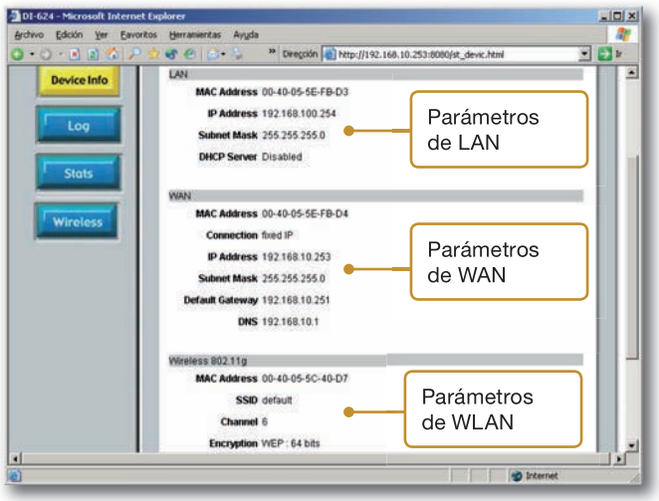


Fig. 7.27. *Página informativa sobre la configuración del encaminador.*

Una vez configurado el encaminador podremos acceder a las páginas de información, en donde podremos comprobar que la configuración seleccionada es correcta (Fig. 7.27).

Conforme las estaciones inalámbricas vayan estableciendo conexiones con el encaminador, su registro de LOG podrá irnos informando de lo que ocurre en la red inalámbrica (Fig. 7.28). Podemos ver que una estación con dirección MAC 00-40-05-30-A6-09 se ha conectado al punto de acceso identificado con el SSID «default» por el canal 6.

Por último, el administrador del encaminador podrá consultar la página de estadísticas de tráfico, de modo que pueda tomar decisiones sobre los cuellos de botella que se generen en el flujo de datos (Fig. 7.29). Podemos ver que las estadísticas están separadas por cada interfaz de red: WAN (flujo hacia o desde Internet), LAN y WLAN (Wireless 11g).

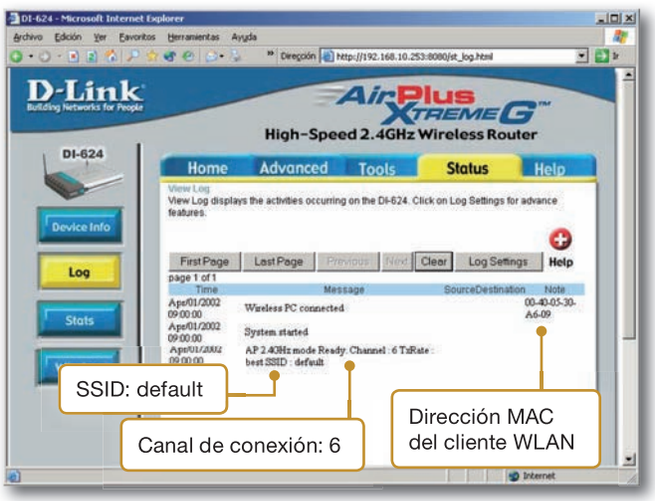


Fig. 7.28. *Visualización del fichero de LOG del punto de acceso del encaminador.*

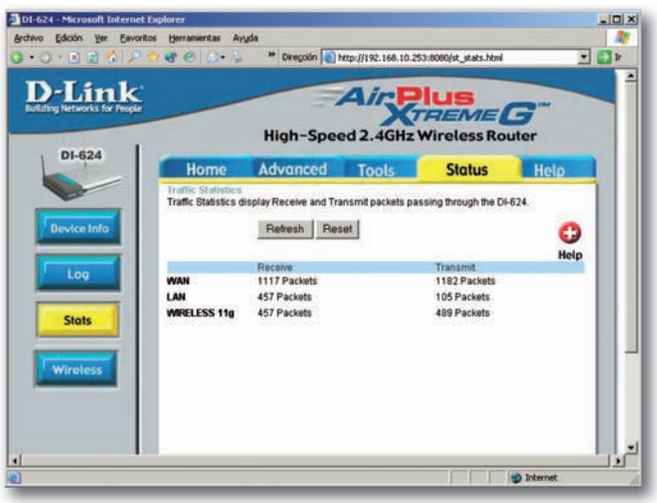


Fig. 7.29. *Página informativa de estadísticas del tráfico en el enrutador inalámbrico.*

Actividades

12. Describe cuáles son los modelos típicos para la integración de redes mixtas.

13. Reconoce la veracidad o falsedad de las siguientes afirmaciones:

a) Los clientes inalámbricos en una red mixta cableada-WLAN no pueden tener el mismo rango de direcciones IP que los clientes de la red cableada.

b) Las redes inalámbricas son siempre redes más inseguras que las redes de cable.

c) El protocolo de encriptación WEP proporciona una seguridad total a la comunicación WLAN.

d) WAP mejora la seguridad frente a WEP.

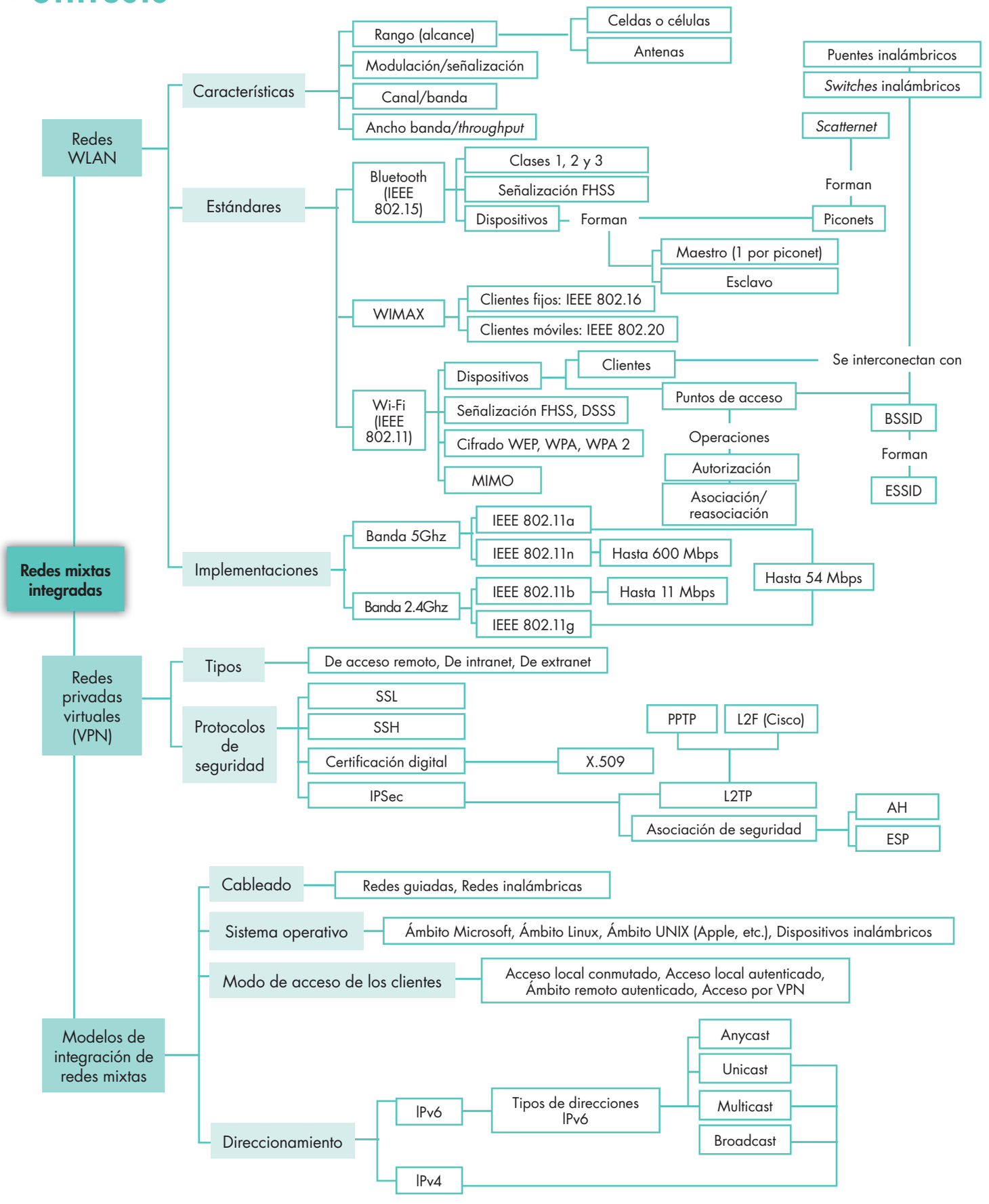
e) El SSID de un punto de acceso identifica el método de seguridad del acceso de los clientes.

14. Debatir en grupo sobre los modelos de integración de redes mixtas sobre las siguientes cuestiones:

a) En una red mixta pueden coexistir nodos Linux y nodos Windows. Estudiar la conveniencia o no de que todos los servidores tengan el mismo sistema operativo (sea Windows o Linux).

b) Sobre la misma red mixta. Estudiar qué ventajas traería que todos los clientes tuvieran también el mismo sistema (sea Windows o Linux).

Síntesis



Test de repaso

1. Enlaza los siguientes elementos característicos de algunas de las tecnologías de redes inalámbricas:

a) Bluetooth	1) Hasta 600 Mbps
b) IEEE 802.11b	2) Hasta 11 Mbps
c) IEEE 802.11g	3) Hasta 54 Mbps
d) IEEE 802.11a	4) Tecnologías MIMO
e) IEEE 802.11n	5) PAN

2. Un dispositivo Bluetooth…

a) Solo puede ser maestro de una única piconet.

b) Solo puede ser esclavo de una única piconet.

c) Puede ser maestro de una piconet y esclavo de otras piconets.

d) Puede ser esclavo de una piconet y maestro de otras piconets.

3. Relaciona los distintos elementos tecnológicos para redes Wi-Fi:

a) WEP	1) IEEE 802.11n
b) WPA/WPA2	2) Cifrado básico
c) SSID	3) Cifrado avanzado
d) Sistema abierto	4) Autenticación en punto de acceso protegido
e) Clave compartida	5) Identificador de un punto de acceso
f) MIMO	6) Autenticación en punto de acceso libre

4. ¿Cuáles de las siguientes afirmaciones son verdaderas?:

a) En una topología inalámbrica *ad-hoc* los nodos se comunican entre sí a través de un punto de acceso.

b) En una topología inalámbrica de infraestructura los nodos se comunican entre sí a través de un punto de acceso.

c) WiMAX se define en el estándar IEEE 802.16.

d) Un conmutador inalámbrico sirve para conectar puntos de acceso entre sí a través de canales de radio.

e) La integración de la Wi-Fi con la red cableada se lleva a cabo mediante los puntos de acceso.

5. Asocia las características tecnológicas sobre IPv4 e IPv6 que aparecen a continuación:

a) IPv4	1) Direcciones unicast
b) IPv6	2) Direcciones multicast
	3) Direcciones anycast
	4) Direcciones broadcast
	5) Direcciones de 128 bits
	6) Direcciones de 32 bits

6. La orden **iwconfig** de Linux se utiliza para…

a) Gestionar la red inalámbrica.

b) Gestionar la red cableada.

c) Gestionar cualquier tipo de red, tanto inalámbrica como cableada.

d) **iwconfig** es una orden de Windows, no de Linux.

7. La dirección «::1» en IPv6 significa…

a) El mismo localhost.

b) La dirección de loopback o de retorno.

c) «Todos los hosts».

d) «Todos los routers».

e) Todos los nodos cuya dirección acaba en «1».

8. Relaciona los elementos tecnológicos que aparecen a continuación sobre redes privadas virtuales.

a) SSL	1) Comunicaciones seguras sobre IP
b) X.509	2) Certificados digitales
c) IPSec	3) Protocolo propietario de Cisco
d) L2TP	4) Protocolo de tunelización sobre PPP
e) L2F	5) Basado en PPTP y L2F
f) PPTP	6) Cifrado de conexiones

9. ¿Cuáles de los siguientes escenarios no son propios de la utilización de IPSec:

a) Comunicación de router a router.

b) Comunicación entre dos cortafuegos.

c) Comunicación de cliente VPN a cortafuegos.

d) Comunicación de *switch* a *switch*.

e) Comunicación de *switch* a router.

10. Relaciona los elementos tecnológicos que aparecen a continuación sobre el modo en que los clientes acceden a la red.

a) Acceso local conmutado	1) Se accede por una red pública creando un túnel
b) Acceso local autenticado	2) RAS sobre protocolo PPP
c) Acceso remoto autenticado	3) IPSec en la LAN o PPPoE
d) Acceso por VPN	4) Utiliza un switch

Solución: 1: a-5, b-2, c-3, d-3, e-(1 y 4); **2:** a y c; **3:** a-2, b-3, c-5, d-6, e-4, f-1; **4:** b, c y e; **5:** a-(1, 2, 4 y 6), b-(1, 2, 3 y 5); **6:** a; **7:** a y b; **8:** a-6, b-2, c-1, d-5, e-3, f-4; **9:** d y e; **10:** a-4, b-3, c-2, d-1.

Comprueba tu aprendizaje

I. Identificar las características funcionales y de configuración de las redes inalámbricas y su relación con la configuración

1. En la primera columna de esta tabla se exponen varias tecnologías. Rellena con SÍ o NO las dos columnas siguientes según la tecnología de la primera columna sea o no aplicable a las redes inalámbricas y a las cableadas.

Tecnologías	WLAN	Red cableada
Dirección IP	Sí	Sí
Máscara de red		
Dirección MAC		
SSID		
Punto de acceso		
Antenas		
WEP		
Conectores de red		
WPA2		
Ethernet		
Wi-Fi		
IEEE 802.11		
IEEE 802.3		

2. Busca los errores en el siguiente argumento técnico:
«Los *hackers* saben muy bien cómo *crackear* una clave WEP. El procedimiento es casi inmediato si la clave WEP es de 64 bits, pero es más difícil si la clave es de 128 bits. Para mejorar la seguridad de las comunicaciones inalámbricas, se ha mejorado WEP con el protocolo WPA, que también funciona con redes cableadas. Todas las comunicaciones que establecen los clientes inalámbricos con el punto de acceso mediante WPA viajan encriptadas por el protocolo SSL.»
3. En la página **http://wifi.cablesyredes.com.ar/html/standards.htm** tienes una comparativa de las prestaciones y características tecnológicas de las tres modalidades de redes IEEE 802.11 (tanto a, b como g). Estudia el mapa tecnológico y piensa un ejemplo sobre cuándo o cómo utilizarías cada tecnología.
4. Monta en el laboratorio un punto de acceso inalámbrico. Después, configúralo del siguiente modo:
   a) Configura la dirección IP del punto de acceso de modo que puedas gestionarlo vía web.
   b) El canal de comunicaciones será el número 8.
   c) La autenticación será abierta, pero la clave WEP será de 64 bits y tendrá el valor «redes».
   d) Configura ahora un cliente inalámbrico de red para que pueda comunicarse con el resto de la red a través del punto de acceso.
5. Configura tres dispositivos que tengan Bluetooth para que puedan comunicarse entre ellos en un área geográfica cercana. Numera los dispositivos como A, B y C.
   a) Configura una piconet entre A-B y otra entre A-C. ¿Quiénes pueden ser maestros y quiénes esclavos?
   b) Ahora haz una piconet donde A sea maestro dejando a B y C como esclavos de A. ¿Puede ser B maestro de otra piconet? En caso afirmativo, ¿de cuál?

II. Identificar los protocolos de cifrado y autenticación utilizados en redes

6. ¿En qué situaciones de las que se exponen a continuación utilizarías VPN y por qué?
   a) Un cliente local accede a un servidor local para recuperar un fichero.
   b) Un cliente remoto accede a un servidor local para imprimir por una impresora compartida.
   c) Un cliente remoto accede a la impresora IPP de un servidor local.
   d) Varios clientes remotos acceden a la vez por una única conexión de Internet a los servicios de una red local.
7. Di si las siguientes afirmaciones son verdad o no:
   a) IPSec es un protocolo de autenticación, pero no de cifrado.
   b) IPSec es un protocolo de cifrado, pero no de autenticación.
   c) IPSec puede encargarse tanto del cifrado como de la autenticación.
   d) L2TP es un protocolo de tunelización para VPN.
   e) Los túneles VPN solo pueden transportar paquetes de redes IP.
   f) VPN es un tipo especial de VLAN.

III. Integrar redes mixtas

8. ¿Qué direcciones IPv6 no son válidas y por qué?
   a) ::10.3.1.1
   b) FF80::<id interfaz>/10
   c) ::1
   d) FE01::10AA::1
   e) FF01::10AA:0001
9. Decide en cada uno de los siguientes casos si conectarías un cliente a la red local a través de una red inalámbrica o a través de una red cableada.
   a) Un cliente envía datos esporádicamente a un servidor local.
   b) Hay un cliente en la red que genera un flujo de datos muy intenso durante algunas horas al día.
   c) Un cliente de red envía datos en tiempo real, pero la densidad de portátiles inalámbricos es muy alta.
   d) Un cliente detecta una docena de células Wi-Fi en su radio de acción.

Práctica final

MUY IMPORTANTE:

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

1. Haber comprendido bien los contenidos de las Unidades 1 a 7 que constituyen los tres primeros bloques temáticos del libro.
2. Haber leído y comprendido el epígrafe 1 de la Unidad final 9, en donde se describe el proyecto del que algunas tareas se resolverán aquí junto con las prácticas finales de los bloques 1 y 2.

En esta práctica de final de bloque configuraremos los equipos de infraestructura de la red en contacto con los usuarios de la misma:

- Conmutadores Ethernet.
- Videocámara IP.
- Punto de acceso inalámbrico.

Truco

Estos tres dispositivos vendrán de fábrica con una dirección IP, usuario y contraseña de administración específicos que podremos averiguar en sus manuales, para que podamos gestionarlos a través de un servidor web. Para comenzar su configuración conectaremos el dispositivo directamente a la interfaz de red de un PC, pondremos en esta interfaz una dirección compatible con la que trae el dispositivo de fábrica y nos conectaremos a él utilizando su dirección mediante el navegador web. Sobre esta página, estableceremos la dirección IP final del dispositivo así como el resto de parámetros de red. A partir de ese momento ya podremos conectar el dispositivo a nuestra LAN y terminar de gestionarlo a través de su dirección definitiva.

1. Configuración de los conmutadores

El conmutador podría configurarse con todos los puertos en la misma VLAN de modo que, aun así, solo se verían entre sí los equipos compatibles por su IP y máscara. Tenemos que configurar dos redes: LAN y WAN. Sin embargo, pensemos qué pasaría si un intruso consiguiera traspasar la barrera del encaminador ADSL: tendría acceso en el nivel 2 de OSI a todas las máquinas puesto que todas estarían en la misma red lógica.

Este problema se soluciona si configuramos dos VLAN, una para la red LAN y otra para la red WAN. De este modo solo dos puertos de un conmutador tendrán que pertenecer a la VLAN de la WAN. Estos dos puertos serían:

1. El puerto por el que se conecta el encaminador ADSL al *switch*.
2. El puerto por el que se conecta IPCOP (el cortafuegos/proxy) en su interfaz WAN al *switch*.

El resto de los puertos del *switch* deberán estar configurados en la VLAN de la LAN, para dar servicio al resto de equipos, incluida la interfaz LAN del cortafuegos.

Si ahora un intruso pasa la barrera del encaminador ADSL (que suelen llevar un sencillo cortafuegos), entonces el intruso tendrá acceso a la red WAN, pero para pasar a la LAN debe saltarse un nuevo cortafuegos: IPCOP. Ya se lo estamos poniendo más difícil al intruso y nuestros clientes de red estarán más protegidos sin perder el acceso a Internet.

Por tanto, vamos a hacer en los conmutadores la configuración de VLAN que se especifica en la Tabla 1.

Conmutador	VLAN/ID	Puertos / Tipo	Observaciones
Eth1 (planta baja)	LAN/1	3-23 / Untag	Rosetas de LAN
IP: 192.168.1.45/24	WAN/2	1-2 / Untag	Router y proxy en planta baja
	LAN/1	24 / Untag	Conexión entre conmutadores
Eth2 (planta alta)	LAN/1	1-23 / Untag	Rosetas de LAN
IP: 192.168.1.46/24	LAN/1	24 / Tag	Conexión entre conmutadores

Tabla 1. *Configuración de niveles 2 y 3 en los conmutadores.*

Práctica final

Obsérvese que los puertos 24 de cada conmutador estarán conectados entre sí para comunicar un conmutador con el otro. Por estos puertos deben pasar paquetes de la VLAN que tiene por ID 1 (que se corresponde con la LAN) ya que en la planta superior no hay ningún dispositivo que se conecte directamente a la WAN. Hemos elegido conmutadores que pueden crear VLAN por puertos.

En la Fig. 1 se ha marcado en naranja lo que está dentro de la VLAN de WAN (que tiene por ID 2 y que en el *switch* real denominaremos también «WAN») y las conexiones de los puntos específicos. Los puertos en azul están dentro de la VLAN de LAN (que tiene por ID 1 y que en el *switch* real denominaremos «default»). El resto de estaciones se pueden conectar a cualquier puerto libre (da igual cuáles sean, pero los que se elijan deben documentarse).

Tenemos que fijarnos en que el paso de paquetes de la WAN a LAN o viceversa solo se puede producir a través del cortafuegos/proxy (IPCOP). La impresora ImpreB2 va conectada al servidor SRV a través de un cable paralelo.

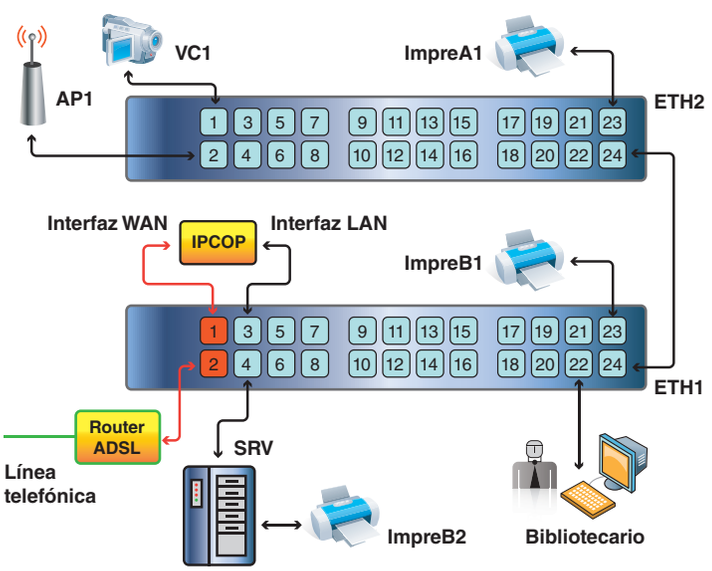


Fig. 1. *Esquema de configuración de los conmutadores.*

CEO

SMR_RL_AAbad_09_Bloque3_Conmutadores.pptx

Documento que contiene información sobre la configuración detallada del conmutador ETH1.

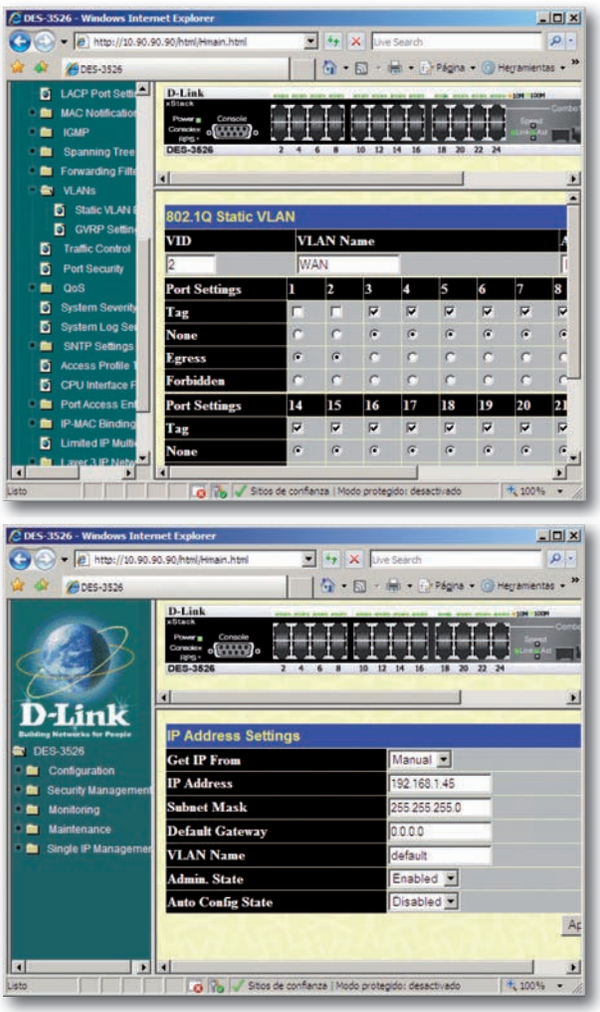


Fig. 2. *Gestión del switch ETH1 mediante su dirección IP (arriba) y gestión de los dos puertos de la VLAN WAN (abajo).*

La Fig. 2 muestra las pantallas de configuración de red local del *switch* ETH1, por donde se gestionará, y la de gestión de VLAN denominada WAN. Primero crearemos todas las VLAN necesarias (en nuestro caso 2), le asignaremos los puertos a cada una de ellas, guardaremos la información en la memoria flash del *switch* y lo arrancaremos de nuevo. A partir de ese momento cualquier equipo que conectemos en los puertos 1 y 2 del primer conmutador estarán en la red que hemos llamado WAN y los que conectemos al resto de los puertos en cualquiera de los dos conmutadores pertenecerán a la VLAN que hemos denominado LAN.

La configuración del segundo *switch* no requiere ninguna intervención puesto que todos los puertos están en la LAN, que es la VLAN que el conmutador trae de fábrica para todos sus puertos.

Práctica final

2. Configuración de la videocámara

La videocámara es un dispositivo que solo exige la configuración de la IP local que vaya a tener. Si se tiene que consultar por Internet, tendremos que configurarle la puerta por defecto para que la información de vídeo sepa salir al exterior. Si no se va a consultar por Internet es mejor no establecer la puerta por defecto porque así nadie podrá robar desde el exterior las imágenes, que es nuestro caso.

El bibliotecario, que conocerá el nombre DNS de la videocámara, podrá acceder a ella a través del explorador web por ese nombre. En la Fig. 3 podemos ver cómo sería la secuencia de configuración de la videocámara, realizada en las instalaciones de PHES.

Fig. 3. *Declaración de los parámetros de red para la webcam VC1.*

3. Configuración del acceso Wi-Fi

El punto de acceso es un dispositivo que aunque tiene dos interfaces de red (la cableada y la inalámbrica) solo tiene que configurarse una dirección IP que compartirán ambas interfaces. Esto nos pone sobre aviso de que el punto de acceso realmente es un concentrador o *bridge* entre la red de radio y la red cableada.

Sin embargo, tenemos que configurar dos elementos diferenciados:

- El interfaz de red, que siempre será local.
- Las condiciones radioeléctricas de la interfaz inalámbrica.

Como otros dispositivos, el punto de acceso suele configurarse a través de su propia página web. Por tanto, una vez que nos hayamos conectado a su servidor web podremos interactuar con sus páginas de administración, que están interrelacionadas mediante un menú web.

3.1. Configuración del punto de acceso

En nuestro proyecto, habíamos definido que los clientes inalámbricos se conectarían mediante Wi-Fi al *backbone* cableado mediante un punto de acceso. En este caso se ha definido que los parámetros de radio son los configurados en la Fig. 4, izquierda, en donde hemos elegido un modo mixto (compatibilidad con clientes b y g) y que el punto de acceso transmitirá su SSID para que los clientes lo identifiquen fácilmente. Los demás parámetros no son relevantes para nuestro estudio.

Además, hemos configurado la transmisión por el canal 5 (Fig. 4, derecha), sistema de autenticación abierto (todos los clientes podrán asociarse al punto de acceso) y clave WEP de 64 bits con el valor «bibli». Esta clave deberá ser suministrada por el bibliotecario a cada usuario inalámbrico para que pueda realizar sus conexiones.

Seguridad

Una medida de seguridad consistiría en que el bibliotecario cambiara esta clave WEP diariamente, de modo que solo se pudiera utilizar la red inalámbrica por quienes conocieran la clave porque hayan pasado previamente por el puesto de recepción del bibliotecario.

Por último, hemos nombrado al punto de acceso con el identificador AP1 y el SSID como «CTT-biblioteca», que será el nombre de red que les aparezca a los clientes inalámbricos cuando exploren el espacio radioeléctrico desde sus portátiles.

Práctica final

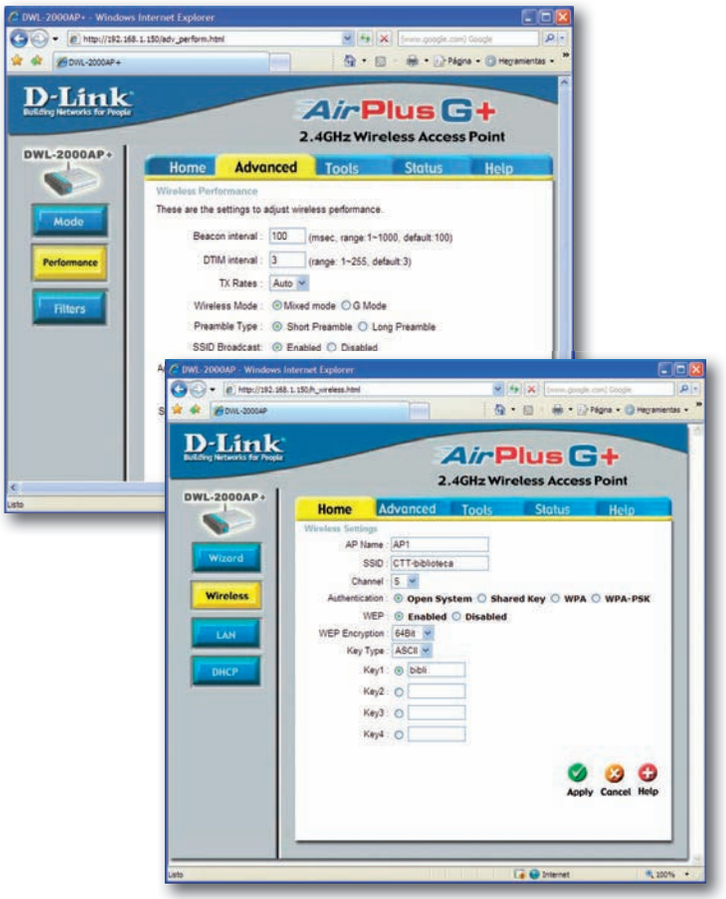


Fig. 4. *Páginas de configuración de la interfaz inalámbrica y el modo de acceso de los clientes en un punto de acceso inalámbrico.*

Fig. 5. *Páginas de administración del servidor DHCP y de la dirección IP local del punto de acceso inalámbrico.*

Generalmente, los puntos de acceso incorporan entre sus prestaciones un servidor DHCP, pero nosotros deberemos deshabilitarlo puesto que ya tenemos uno configurado en la LAN sobre SRV de mucha más potencia (Fig. 5, izquierda).

Por último, solo faltaría terminar de cambiar la dirección IP local del punto de acceso para que cumpla las especificaciones del proyecto en donde AP1 tenía que tener como dirección 192.168.1.43/24 (Fig. 5, derecha).

Obsérvese que no hemos especificado la puerta por defecto *(Gateway)*. La razón es que el punto de acceso como tal no tiene que salir a Internet (no decimos los clientes inalámbricos que utilizan el punto de acceso, sino el mismo punto de acceso que no deja de ser un nodo más de la red). Si quisiéramos administrar el punto de acceso desde el exterior, tendríamos que rellenar el campo de *Gateway* apuntando a 192.168.1.100 y publicar la página de administración del punto de acceso en los cortafuegos.

Truco

Algunos dispositivos no permiten que el *Gateway* quede vacío. En estos casos, dejar este campo vacío es equivalente a rellenarlo con la misma dirección IP que tiene el dispositivo que se configura (en el caso del punto de acceso: 192.168.1.43).

3.2. Configuración de los clientes inalámbricos

En el caso de los clientes inalámbricos tendremos que conseguir unas características de red compatibles con las que hemos definido en el punto de acceso. Esto quiere decir que se podrán conectar a la red local mediante radiofrecuencia aquellos equipos que cumplan las siguientes características:

1. Deberán utilizar tecnología Wi-Fi en sus versiones a o g, que son las que permite el punto de acceso configurado.
2. El punto de acceso no les ofrecerá ningún obstáculo para asociarse a él puesto que su modo de autenticación es abierto *(open)*.

Práctica final

3. Tendrán que cifrar las comunicaciones mediante WEP de 64 bits y además tendrán que conocer esta clave WEP, que ha sido establecida inicialmente como «bibli».
4. Tendrán que configurar su nivel 3 de red como clientes DHCP, para que el servidor DCHP instalado en SRV les proporcione a través del punto de acceso su dirección IP de cliente. Daremos más detalles sobre el modo de hacerlo en la Unidad 9 cuando se detallen las configuraciones de las estaciones cliente.

No olvidemos que en ese DHCP definimos un ámbito de direcciones IP para los clientes inalámbricos que suministraba a los clientes DHCP mediante petición la dirección IP en el rango 192.168.1.51 a 192.168.1.70, la máscara 255.255.255.0 y el servidor DNS 192.168.1.10, justo unos parámetros compatibles con el resto de la red LAN.

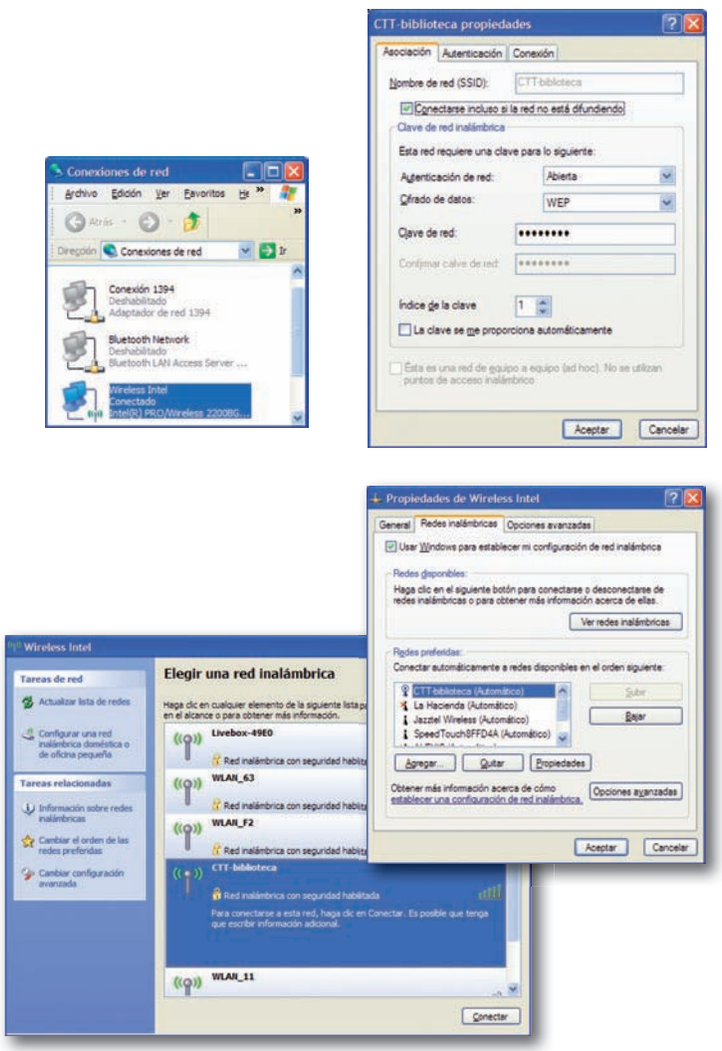


Fig. 6. *Configuración del acceso inalámbrico en un nodo Windows.*

Si abrimos las conexiones de red (Fig. 6) en Windows, podremos ver la interfaz inalámbrica. En sus propiedades, podremos explorar el espacio radioeléctrico a la búsqueda de redes disponibles (los SSID a nuestro alcance). Vemos en la figura que tenemos disponible la red CTT-biblioteca, que es la del punto de acceso configurado. Si volvemos a propiedades de la interfaz inalámbrica podremos ver las propiedades de las redes inalámbricas, dejando que Windows configure automáticamente la red. Podremos ver la red a la que nos queramos conectar y procederá a realizar la conexión. En las propiedades de cualquier red inalámbrica seleccionada podremos configurar el resto de los parámetros de conexión como el sistema de autenticación en el punto de acceso o la clave WEP, aunque, si no se rellena, cuando el cliente hace la conexión la solicitará al usuario.

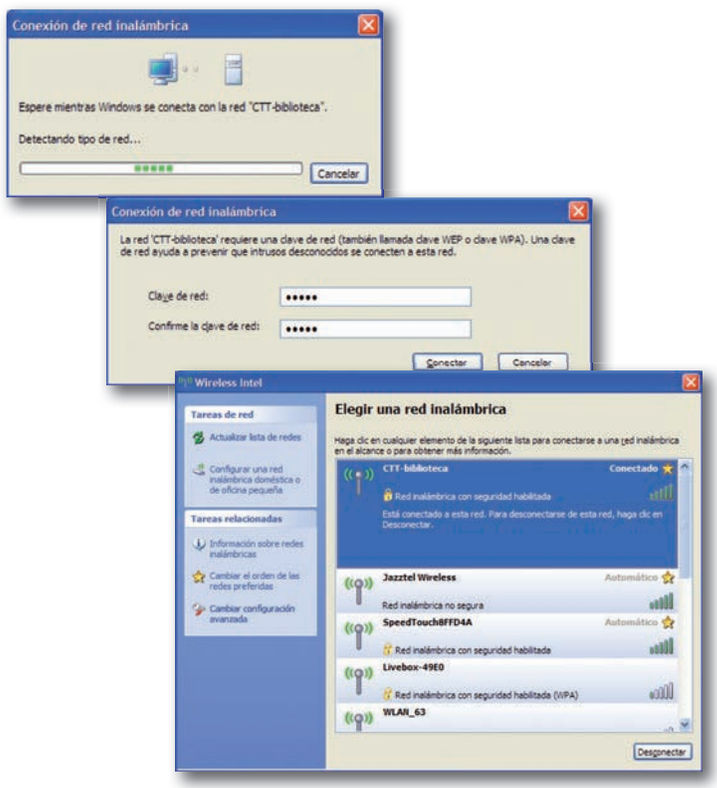


Fig. 7. *Conexión a la red inalámbrica en Windows.*

Al intentar realizar la conexión (Fig. 7), el nodo se da cuenta de que el punto de acceso está protegido mediante una clave WEP y, si no la configuramos en la ficha de propiedades de la red, nos la pedirá (Fig. 7, centro). Si acertamos con la clave, se realizará la conexión y, a partir de ese momento, nuestro nodo inalámbrico empezará a formar parte de la LAN.

Una nueva exploración de las redes inalámbricas nos indicará que efectivamente estamos conectados a la red elegida (Fig. 7, derecha).

Práctica final

En el caso de clientes Linux, el modo de operación es semejante.

Podemos explorar las redes inalámbricas disponibles, seleccionamos una de ellas, rellenamos los parámetros de conexión, dejamos que DHCP haga todo el trabajo de direccionamiento IP y se procederá a realizar la conexión.

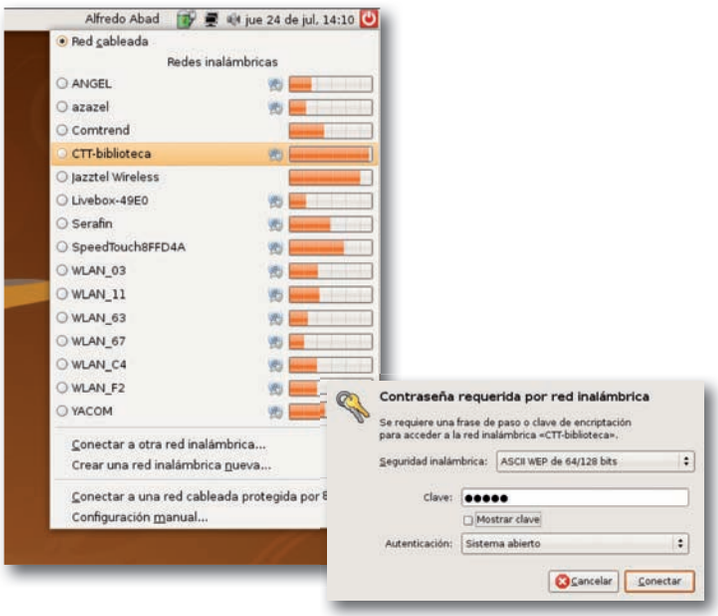


Fig. 8. *Detalles de la conexión inalámbrica en un cliente Linux.*

En la Fig. 8 (izquierda) podemos ver un detalle del escritorio Ubuntu en donde estamos explorando el espacio radioeléctrico, lo que se consigue en el icono de redes que aparece en el panel superior.

Una vez que hemos elegido la red a la que deseamos conectarnos se realizará el intento de conexión y nos pedirá la clave WEP (Fig. 8, derecha) junto con sus características (64 bits en nuestro caso).

Si tenemos éxito, se validará la conexión y ya estaremos en la red de área local.

Fig. 9. *Visualización de la configuración de la conexión inalámbrica una vez aceptada por el punto de acceso.*

Si ahora pasamos el ratón por encima del icono de redes (en la barra superior) nos indicará con un globo informativo a qué red estamos conectados (Fig. 9, arriba) junto con la cobertura de que disponemos.

Del mismo modo, la orden **iwconfig** nos indicará los parámetros de conexión utilizados en la asociación al punto de acceso (Fig. 9, abajo).

Como en todos los casos, la configuración del direccionamiento IP para esta interfaz inalámbrica será la de DHCP o modo itinerante.

CEO

SMR_RL_AAbad_09_Bloque3_Wi-Fi.pptx
Documento que contiene información sobre:
1. Configuración del punto de acceso AP1.
2. Configuración de un cliente inalámbrico Windows.
3. Configuración de un cliente inalámbrico Linux.

Unidad 8

Protección, vigilancia y soporte de redes

En esta unidad aprenderemos a:

- Entender la necesidad de seguridad en la red proponiendo modos de filtrado que garanticen la legalidad y las actuaciones éticas.
- Identificar las actuaciones de vigilancia y soporte de la red.
- Documentar la red.

Y estudiaremos:

- Los distintos sistemas de filtrado aplicables a la red.
- Los principios de deontología profesional.
- Los documentos que recogen el mapa de red.

CEO

SMR_RL_AAbad_08_DirectivaSeguridad.docx

Documento que contiene información sobre políticas de seguridad.

Seguridad

El administrador no debe permitir indiscriminadamente cualquier tráfico de datos por la red que administra. Por ella solo debe circular la información que sea estrictamente necesaria; en caso contrario, penalizaría el ancho de banda de la red disponible y además facilitaría que, en el mejor de los casos, los usuarios de la red pudieran perder su tiempo entreteniéndose en actividades para las que no han sido autorizados. Otras veces, la limitación del tráfico viene aconsejada por la lucha contra el intrusismo y los virus o códigos maliciosos.

CEO

SMR_RL_AAbad_08_NecesidadSeguridad.docx

Documento que contiene información sobre:

1. Necesidad de la seguridad.
2. Cifrado electrónico.
3. Firma electrónica.

Seguridad

Es importante, además de obligatorio, respetar la legislación concreta de cada país de modo que se puedan arbitrar mecanismos de censura de la información y hacerlo compatible con el derecho a la información que tienen todas las personas.

1. El filtrado de la red

Las redes incrementan notablemente la funcionalidad de los ordenadores, permitiéndoles cooperar entre sí. Muchas aplicaciones de red soportan gran parte de la carga de trabajo de las corporaciones en donde están instaladas, de modo que hay que asegurar su correcto e ininterrumpido funcionamiento, especialmente en tareas de misión crítica.

Junto con ello, hay que asegurar que los datos son accesibles por quienes deben procesarlos y solo por ellos. En caso contrario, perderíamos la confidencialidad y nos haríamos más sensibles al intrusismo. Todo esto exige una firme apuesta por la seguridad.

La seguridad de la red sigue un plan completamente definido y aprobado por todas las instancias de la empresa con capacidad de decisión. Cuando la red es grande, se puede establecer un departamento especializado en la seguridad separado de los departamentos de redes o de sistemas, aunque lo habitual es que la seguridad esté integrada en los departamentos encargados del despliegue y de mantenimiento.

En las normas de seguridad informática y de comunicaciones de las empresas podemos encontrar directivas del estilo siguiente:

- Los equipos deben protegerse con seguridad física contra robos.
- El acceso físico a los servidores estará restringido a los administradores de la red, es decir, ningún usuario de la red podrá entrar en las salas en donde se instalan los servidores.
- No se permite la descarga de aplicaciones o utilidades desde Internet.
- No está permitida la instalación de aplicaciones de las que no se tenga licencia.
- Las contraseñas de los usuarios tienen que sobrepasar un determinado nivel de dificultad.
- Cuando un usuario se equivoque al presentarse en el sistema un número de veces concreto, el sistema bloqueará la cuenta, que deberá ser desbloqueada por el administrador.
- Cualquier portátil que se conecte a la red deberá tener actualizado y activo su antivirus, en caso contrario se le denegará el acceso a la red.

Las normas de seguridad de obligado cumplimiento que atañen al software y las comunicaciones suelen implantarse en los sistemas mediante directivas de software, también denominadas políticas de seguridad.

1.1. Filtrado de contenidos web

La empresa que sostiene una instalación de red decide qué informaciones pueden circular por ella. El administrador de red, en nombre de la compañía, debe limitar la información que entra en su red a través de Internet para evitar contenidos indeseados y que su red no sirva como medio para cometer delitos o acciones deshonrosas que puedan hacer daño a la empresa, a su imagen o a terceras personas.

Actualmente, los filtros de contenidos de Internet acuden a tres técnicas básicas:

1. La primera de ellas consiste en reconocer en la información transmitida las palabras para compararlas con una lista de palabras prohibidas. Cuando la información contiene alguna de las palabras no permitidas, se deniega el acceso a la página. Este método es muy rudimentario e ineficaz, pues frecuentemente las páginas se hacen indeseadas por análisis del contexto en que las palabras aparecen. Por ejemplo, si limitamos la palabra «sexual», no sabremos si se trata de una página pornográfica o de un ensayo científico.

Vocabulario

Aplicar un filtro a una comunicación: consiste en evaluar la comunicación por comparación con un patrón de referencia que la permite o la impide. A este patrón se le denomina directiva del filtro.

2. El segundo método se basa en la utilización de listados de sitios prohibidos que han sido previamente clasificados por la empresa que nos suministra el filtro. El problema de este método reside en que las páginas de Internet cambian con frecuencia y no hay una manera razonable de tener las listas actualizadas. Además, un sitio puede tener información válida y no válida simultáneamente. El filtro, por este método, nos denegaría el acceso a toda la información del sitio web, también a las páginas lícitas.
3. El tercer método es muy eficaz, pero utópico. Las páginas web pueden ser etiquetadas de modo que el explorador convenientemente configurado rechace las páginas con ciertas etiquetas. El problema que tiene este método es que todas las páginas web deberían estar etiquetadas, lo que no ocurre realmente. Microsoft Internet Explorer (Fig. 8.1) es compatible con esta tecnología, que se denomina PICS.

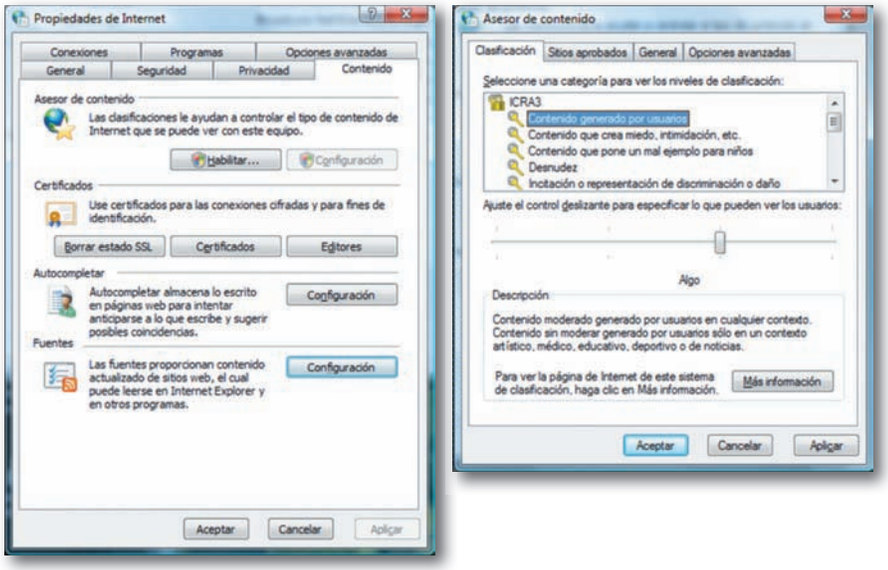


Fig. 8.1. *Configuración del acceso a contenidos en Internet Explorer sobre Windows Vista.*

Ejemplos

Instalación del filtrado de servidor de Optenet

Como ejemplo, vamos a ver la configuración de Optenet, uno de los filtros de contenidos más populares. Optenet se sirve en dos opciones, una opción de cliente y otra de servidor. Como cliente, Optenet se instala en cada PC de modo que cualquier petición de página web es filtrada por el software de Optenet. El filtro actualiza sus listas con la frecuencia que le digamos. Existen versiones de Optenet también para sistemas Linux.

En su versión de servidor, Optenet se instala sobre un servidor proxy. Si no disponemos de este servidor, Optenet instala uno propio. El funcionamiento del filtro de servidor es similar al filtro de cliente, pero en la versión de servidor un único filtro atiende a todos los usuarios que se conectan al proxy.

La instalación de Optenet se realiza sin problemas. El único dato algo especial que solicita la instalación es si tenemos o no un servidor proxy sobre el que poner el filtro y, en caso negativo, si queremos que Optenet ponga su propio proxy.

Una vez realizada la instalación sobre un servidor, Optenet crea un servidor web para que, mediante el explorador, podamos configurarlo. En nuestra instalación de ejemplo, el filtro se ha instalado sobre un sistema Windows Server 2003 con Microsoft ISA Server como servidor proxy.

Desde el menú de inicio de Windows ejecutamos la página web de Administración de Optenet y nos pedirá una identificación de administrador del filtro para posteriormente enseñarnos la página de administración.

La página de configuración nos permite activar o parar el filtro e indicarle la información que queremos recoger en un fichero log, que se situará en los directorios de instalación del filtro, pero que puede cambiarse a cualquier otra ubicación.

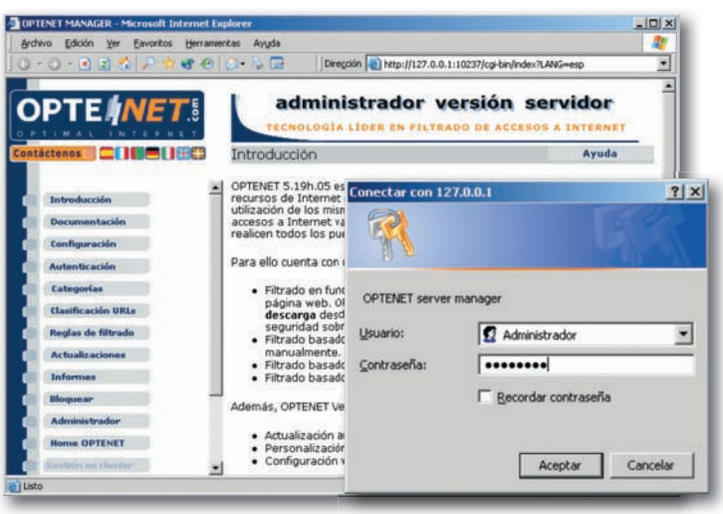


Fig. 8.2. *Arranque de la página web de configuración de Optenet.*

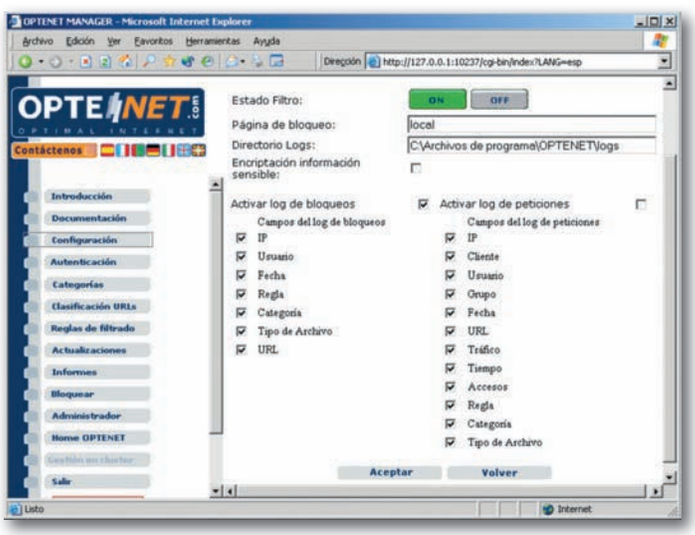


Fig. 8.3. *Página de configuración de Optenet.*

Continúa...

Ejemplos

...Continuación

En la página de autenticación (Fig. 8.4) podemos indicarle a Optenet quiénes son los usuarios de la red, de modo que después se puedan crear políticas de acceso en función de los usuarios. Por ejemplo, al departamento financiero se les puede dejar leer la prensa, algo que carece de sentido para el personal de almacén.

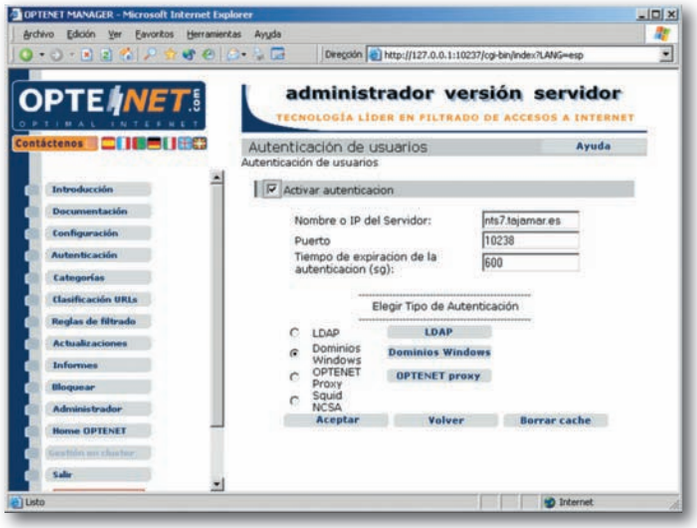


Fig. 8.4. *Página de autenticación de Optenet.*

Optenet se integra en el Directorio Activo de Microsoft, de modo que los usuarios de los dominios de Microsoft son también los usuarios de Optenet.

En la página de clasificación de URL, Optenet permite que el administrador del filtro modifique las propias listas de filtrado, de modo que se establecen listas por categorías en las que se permite el acceso porque se consideran webs seguras o se deniega el acceso si el contenido no es conveniente.

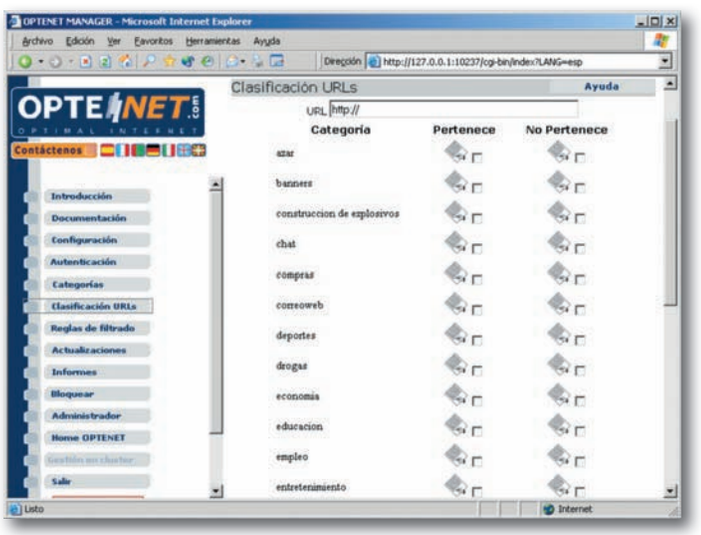


Fig. 8.5. *Página de clasificación de URL de Optenet.*

En la página de reglas de filtrado se establecen las políticas de acceso, es decir, se define quién puede acceder desde dónde para obtener qué contenidos. Si la condición se cumple, Optenet servirá el contenido solicitado al usuario, pero si no se cumple, el acceso quedará denegado y se escribirá un registro en el fichero de log del filtro para información del administrador y el control estadístico. En esta información de log aparecerá reflejada la regla que se ha violado y que ha causado la denegación de servicio.

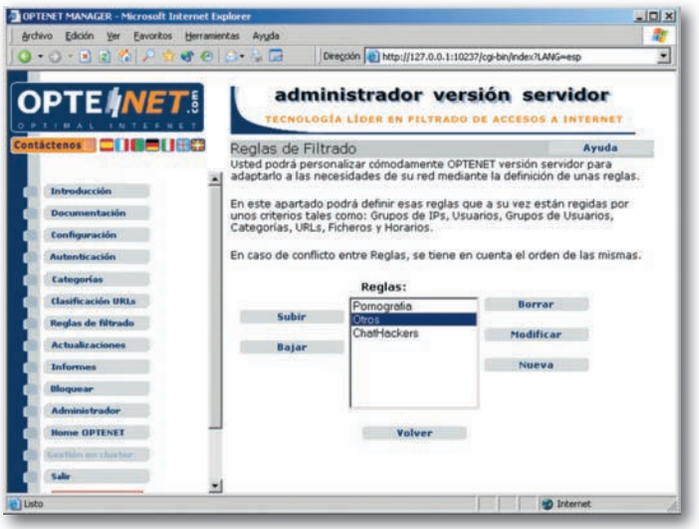


Fig. 8.6. *Página de reglas de filtrado de Optenet.*

La ficha de actualizaciones nos permitirá configurar cómo se actualizan las listas de Optenet. Básicamente podemos decirle a Optenet la periodicidad de la actualización y a qué horas esta se permite. Lo habitual es que la actualización se haga por la noche para que el filtro no consuma el ancho de banda de los navegantes durante su trabajo por el día.

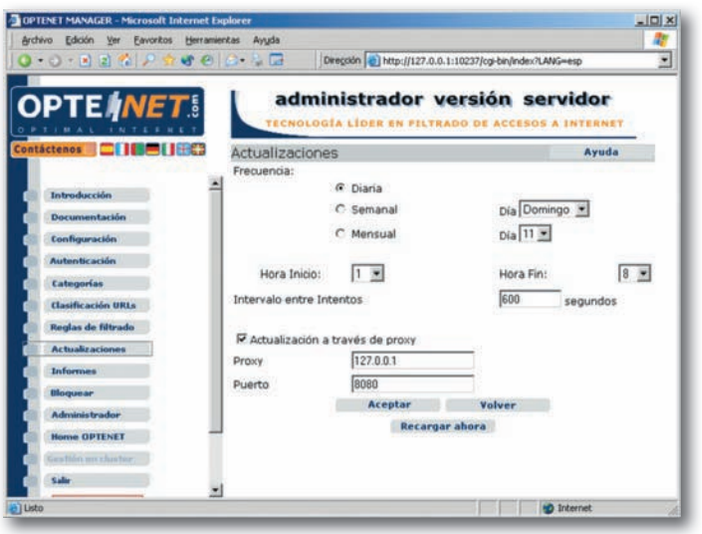


Fig. 8.7. *Página de actualizaciones de Optenet.*

Continúa...

Ejemplos

...Continuación

Además, en esta página podemos indicarle a Optenet que utilice un proxy para buscar la actualización en Internet. Obsérvese que en la Fig. 8.7 la dirección IP del proxy es 127.0.0.1, que es la dirección reservada para la misma máquina en que está instalado el filtro. Tenemos que recordar que, en nuestra instalación de ejemplo, el filtro e ISA Server están instalados en el mismo servidor.

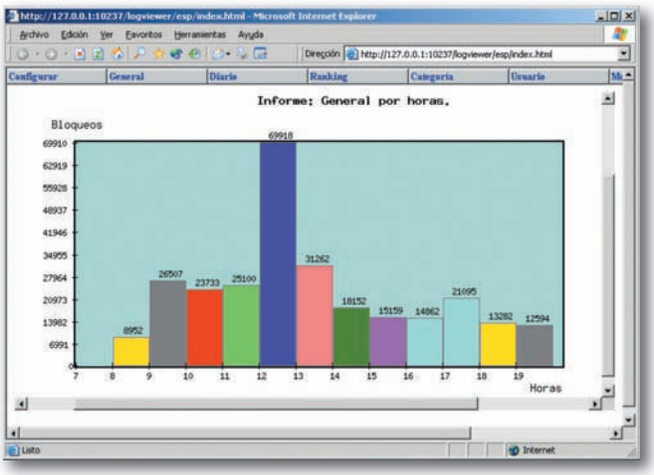


Fig. 8.8. *Gráfico estadístico de la actividad de Optenet.*

En la Fig. 8.8 podemos ver un gráfico de barras que muestra la actividad de Optenet. El administrador puede configurar los formularios para la realización de informes gráficos sobre lo que ocurre en la red con los accesos a Internet.

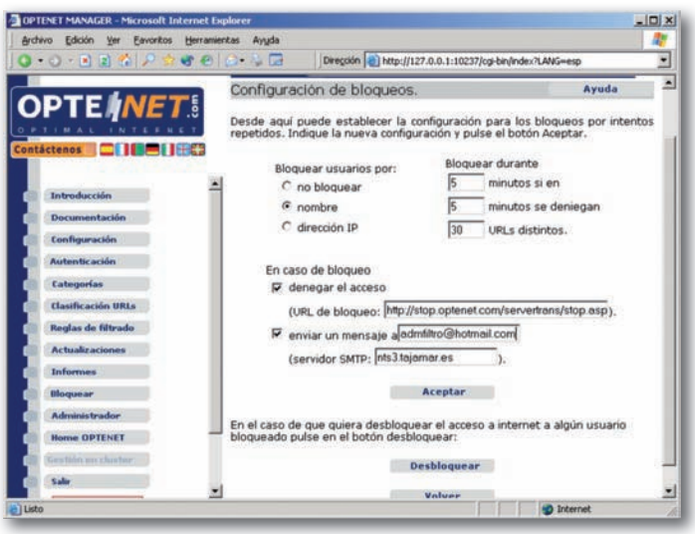


Fig. 8.9. *Página de definición de bloqueos de Optenet.*

En la página de definición de bloqueos podemos indicar al filtro que nos avise mediante correo electrónico cuando detecte una actividad no permitida que exceda unos umbrales, de modo que se pueda denegar el acceso durante un tiempo determinado, pasado el cual, Optenet volverá a liberar la conexión del usuario.

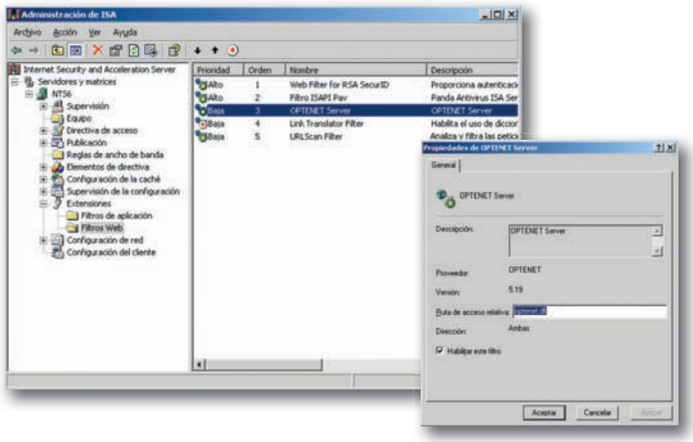


Fig. 8.10. *Vista de Optenet desde la consola de administración de Microsoft ISA Server.*

Por último, en la Fig. 8.10 podemos ver cómo ve ISA Server al filtro y cómo este filtro también se puede activar o desactivar desde ISA Server.

Cuando ISA Server recibe una petición de acceso web desde un usuario de la red corporativa, llama al filtro para que este determine si el acceso está o no autorizado en función de las políticas definidas por el administrador del filtro.

Si el acceso no viola ninguna de las políticas definidas, entonces ISA Server recuperará la página solicitada desde Internet o desde su propia caché de páginas web.

Sin embargo, si alguna o varias políticas se infringen, entonces el filtro presentará al usuario un mensaje de denegación de servicio.

En la Fig. 8.11 hemos intentado acceder a la página web de una revista de información rosa a través del filtro de Optenet.

El administrador del filtro ha creado una política denominada «rosa» que impide que el usuario que intenta acceder a la web consulte periodismo rosa.

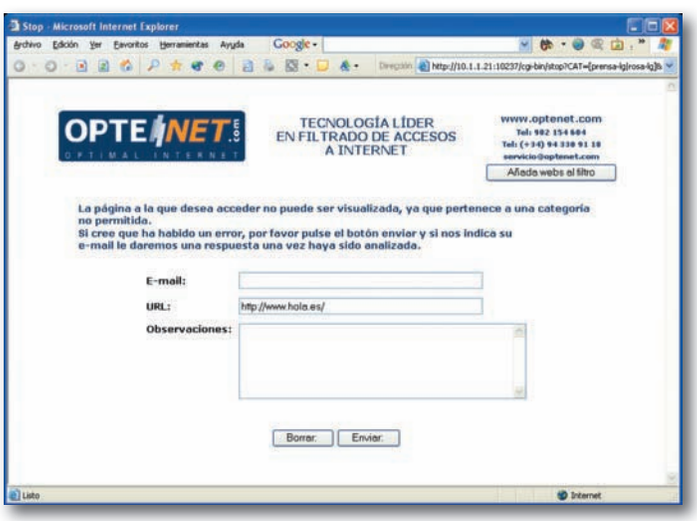


Fig. 8.11. *Página de denegación de servicio de Optenet.*

1.2. Filtrado de correo

El filtrado de contenidos no solo afecta a las páginas web. Es común filtrar los contenidos de los correos electrónicos. Por ejemplo, el administrador del servidor de correo de la red podría filtrar los correos que vinieran de ciertos remitentes porque se considera inseguro el contenido que de ellos procede.

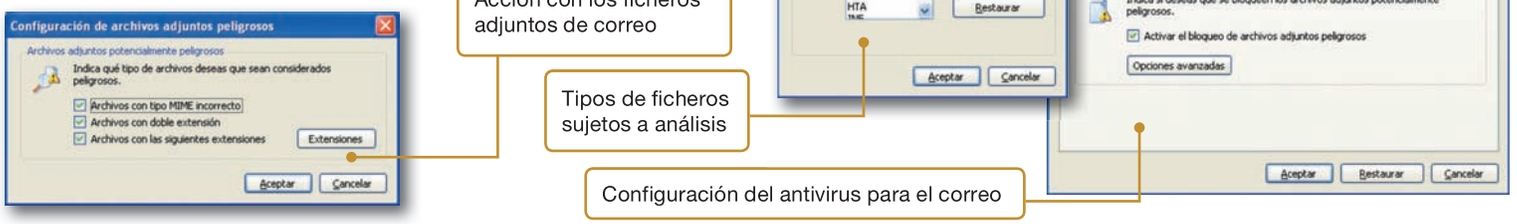


Fig. 8.12. *Configuración de análisis de virus en correo electrónico de un conocido antivirus.*

En la Fig. 8.12 vemos las ventanas en secuencia de la configuración del análisis de correo electrónico para un antivirus. Además de activarlo o desactivarlo, podemos indicarle al antivirus que queremos analizar solo correo de entrada, de salida o ambos, e incluso en los ficheros adjuntos comprimidos, con algunas extensiones o para todas las extensiones de ficheros.

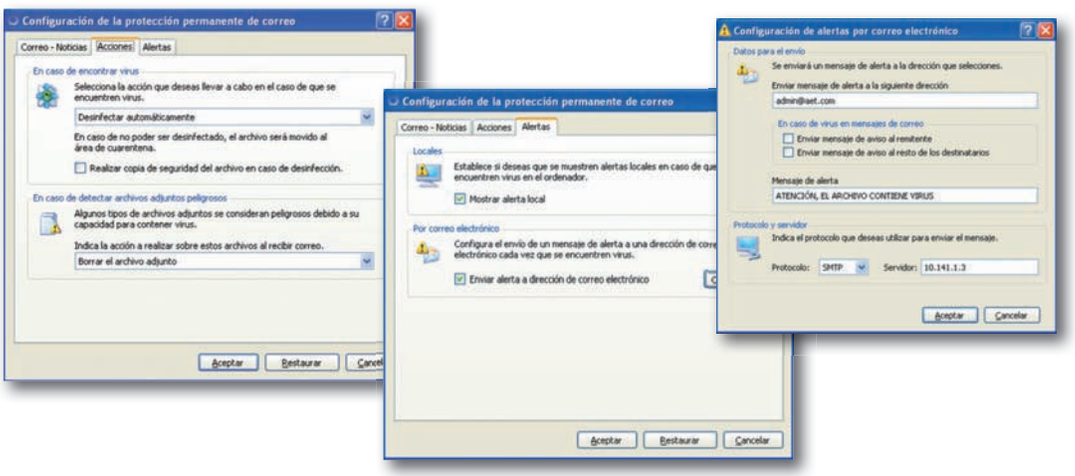


Fig. 8.13. *A la izquierda, definición de acciones a realizar con los correos electrónicos infectados. A la derecha, fichas de configuración de alertas en un antivirus.*

Posteriormente tendremos que definir qué hacer con los correos electrónicos que lleguen al sistema y que estén infectados por algún virus: podemos eliminarlos, desinfectarlos, ponerlos en cuarentena, etc.

Por último, podemos establecer las alertas con las que nos avisará el antivirus de que ha detectado un virus en un correo. Podemos indicarle que nos avise mediante un mensaje o que nos envíe un correo electrónico a una dirección de administración. En este caso, tendremos que decirle cuál es el servidor de correo electrónico al que tendrá que enviar el correo de aviso.

Investigación

Busca información en Internet sobre diversos tipos de filtrado de páginas web para que te familiarices con los servicios que proporcionan. Puedes empezar tu búsqueda por **http://www.consulintel.es/Html/Productos/Cacheflow/filtrado.htm**

Otra página de interés sobre protección de menores es **http://cert.inteco.es/Proteccion/Menores_protegidos/Para_padres_y_educadores/**

Seguridad

Sería muy arriesgado que las entradas de correo electrónico al servidor de correo corporativo no estuvieran filtradas por un buen sistema antivirus. Esto implica que todo correo electrónico debe ser analizado minuciosamente en busca de código malicioso. Los programas de antivirus descomprimen incluso la información que viene comprimida.

CEO

SMR_RedesLocales_08_ConfiguracionAntivirus.pptx

Presentación PowerPoint con diapositivas autoexplicativas sobre los elementos que permiten la configuración completa de una suite de antivirus (Panda Internet Security 2011).

Claves y consejos

La configuración de las políticas de routers y *firewalls* es uno de los puntos más difíciles para el administrador de la red y, además, de los más críticos para la seguridad.

1.3. Filtrado de conexiones

Por seguridad, puede hacerse interesante impedir que ciertas máquinas de la red se conecten a servidores concretos. De este modo, solo dispositivos autorizados podrían utilizar los servicios que el servidor provee en los distintos puertos de conexión. Este modo de limitar quién se conecta a dónde se denomina filtrado de conexiones.

La mayor parte de los encaminadores tienen esta función además de la suya específica, que es el enrutamiento de los paquetes. Es evidente que todos los cortafuegos también lo tienen, puesto que esta es precisamente su función específica.

Los cortafuegos y encaminadores realizan esta función definiendo políticas de acceso.

1.4. La seguridad en la red

Teniendo en cuenta que muchas redes se conectan a Internet a través de dispositivos que las ocultan, la cifra de ordenadores que pueden volcar datos a Internet es gigantesca. Lo que a nosotros nos interesa ahora es que la inseguridad de nuestro sistema puede venir, entre otros factores, por cualquiera de esos nodos de la red.

Cuando se planifica la seguridad de una red hay que tener en cuenta:

- La seguridad y la complejidad suelen guardar una relación de proporcionalidad inversa, es decir, a mayor seguridad se simplifican los procedimientos, ya que la seguridad es limitadora de las posibilidades. Además, la educación de los usuarios de la red debe ser lo más intensa posible.
- La seguridad y la facilidad de uso suelen guardar frecuentemente una relación de proporcionalidad inversa; por tanto, resulta conveniente concentrarse en reducir el riesgo, pero sin desperdiciar recursos intentando eliminarlo por completo, lo que es imposible.
- Un buen nivel de seguridad ahora es mejor que un nivel perfecto de seguridad en un futuro incierto. Por ejemplo, se pueden detectar diez acciones por hacer; si, de ellas, ahora lleva a cabo cuatro, su sistema será más seguro que si espera a poder resolver las diez.
- Es mejor conocer los propios puntos débiles y evitar riesgos imposibles de cuantificar.
- La seguridad es tan potente como su punto más débil, por tanto, interesa centrarse en las debilidades más acusadas.
- Lo mejor es concentrarse en amenazas probables y conocidas.
- Aunque la seguridad conlleva un gasto para la empresa, debe ser considerada como una inversión.

CEO

SMR_RL_AAbad_08_FiltradoInformacion.docx

Documento que contiene información sobre:

1. Filtrado de información de entrada en la red.
2. Filtrado de conexiones por protocolos.
3. Protección del sistema con antivirus.
4. Protección contra accesos indebidos.

Claves y consejos

Al plantearse el diseño de la seguridad de la red hay que seguir una serie de pasos, como evaluar los riesgos que corremos, definir la política fundamental de seguridad de la red, cómo se diseñarán las tácticas de seguridad, tener previstos unos procedimientos de incidencias-respuesta, etc.

CEO

SMR_RL_AAbad_08_OPTENET Security Suite.pptx

Presentación PowerPoint con diapositivas autoexplicativas sobre la instalación y configuración de *Optenet Security Suite.*

Actividades

1. Analiza la veracidad o falsedad de las siguientes afirmaciones, razonando las respuestas:

a) Siempre que el asaltante de un equipo en red no tenga acceso físico al mismo, el sistema estará seguro.

b) Un sistema está seguro porque el asaltante no tiene acceso por red aunque tenga acceso físico al equipo.

c) El antivirus protege totalmente de virus.

d) Un sistema de filtrado de contenidos de páginas web impide con una alta probabilidad el acceso a páginas no permitidas por el administrador de red.

2. Descarga de la web de Optenet **(www.optenet.com)** la versión cliente de prueba de su filtro Optenet. Prepara un PC con una conexión a Internet y comprueba que puedes acceder a los servicios de navegación. Seguidamente, instala el filtro de Optenet y configúralo con la ayuda de la guía de usuario. Comprueba su funcionamiento.

3. Descarga desde Internet alguna suite de seguridad de algún proveedor de antivirus. Pueden servirte las versiones de demostración que no requieren pago de una licencia durante el periodo de pruebas. Instálalo en una estación y prueba a descargar EICAR. Comprueba que el antivirus detecta la descarga como un virus.

4. Intenta aprender algo más sobre cómo funcionan los sistemas de filtrado de contenido investigando los métodos que utilizan para hacer su función. Como resultado de tu trabajo puedes confeccionar un mapa conceptual sobre ello. Puedes empezar a buscar información a partir de la página **http://funnix.net/tecnologia/2011/filtros-web-parte-i/ o de http://www.eldeber.net/progfiltro.htm**

2. Vigilancia y mantenimiento de la red

Entramos ahora en lo que es la vida diaria del administrador de red. Ocasionalmente, el administrador debe realizar nuevas instalaciones por ampliaciones de la red, por actualizaciones de la red existente o porque deben cambiarse los equipamientos debido a su alta obsolescencia tecnológica. Estas actuaciones extraordinarias son las que constituyen la función de **despliegue.**

Sin embargo, lo habitual y ordinario es un servicio de asistencia tanto a los equipos, lo que llamaremos mantenimiento, como a los usuarios de los mismos, es decir, al soporte.

2.1. La continuidad del servicio de red

Cuando se realiza una inversión en la instalación de una red de ordenadores, se prevén las amortizaciones por un periodo de tiempo concreto que varía dependiendo de los elementos de la red que se considere. Por ejemplo, los sistemas operativos podrían sustituirse en periodos que van de dos a cuatro años. El sistema de cableado es mucho más duradero: las líneas troncales pueden durar más de diez años, mientras que el cableado horizontal deberá actualizarse conforme progresen las futuras obras de acondicionamiento del edificio. Los dispositivos de red pueden explotarse entre cuatro y ocho años.

Aunque cada elemento tiene un periodo de caducidad distinto, la realidad es que la corporación que instala la red necesita continuidad en los servicios prestados por la red, con independencia de si el administrador está en proceso de sustituir alguna parte de ella; es decir, una red debe ser operativa durante todo su ciclo de explotación previsto cuando se realizó la inversión.

Estas actualizaciones o nuevas instalaciones exigen paradas en el servicio. Estas paradas deben estar previstas en la medida de lo posible para que se produzcan durante los tiempos de menor carga productiva, de modo que el impacto económico de las paradas sea mínimo. Además, los usuarios de los servicios que se van a detener deben ser avisados y, si es posible, aconsejarles vías alternativas para la realización de su trabajo.

Hay que poner especial cuidado en la previsión de paradas en aquellos servidores que soportan las **aplicaciones de misión crítica.**

Hay paradas que no se podrán prever, como las paradas derivadas de averías imprevisibles. Para estos casos, el administrador debe tener previstos procedimientos de reparación que tengan el menor impacto posible, por ejemplo, manteniendo repuestos de los componentes críticos más importantes o que tengan una mayor probabilidad de avería, proponiendo hardware redundante, etc.

Ocasionalmente, las empresas contratan con sus proveedores de servicios actuaciones de mantenimiento y soporte con unas condiciones económicas tan exigentes como sean capaces de pagar, de modo que se pueden dedicar a su negocio dejando para esos proveedores lo que es específicamente tecnológico. A estos servicios contratados con terceras partes se les llama ***outsourcing.***

En otros casos, las redes empresariales no poseen los servidores de misión crítica, sino que se realizan contratos con otras empresas que proveen no ya el soporte y mantenimiento, sino también el propio servicio informático y de comunicaciones. Por ejemplo, estos proveedores pueden tener en sus instalaciones los servidores de sus empresas-cliente. En el caso de los proveedores telemáticos, esto suele ocurrir siempre, puesto que se trata de servicios de comunicación que no tienen una localización geográfica, sino que se extienden a toda una red de transporte. En estos casos, los clientes suelen firmar acuerdos de continuidad del servicio con sus proveedores (acuerdos SLA, *Service Level Agreement*).

Un acuerdo SLA puede especificar, por ejemplo, que los servicios que tenga contratados estarán disponibles por encima del 99,99 por ciento del tiempo. Si el proveedor no es capaz de respetar los términos del acuerdo, deberá atenerse a las cláusulas punitivas del contrato.

Vocabulario

Despliegue: se suele denominar despliegue al conjunto de acciones que permiten la instalación progresiva de un sistema distribuido de sistemas y aplicaciones.

Vocabulario

Aplicaciones de misión crítica: son aquellas que no pueden dejar de funcionar sin un gran impacto sobre la producción global de la empresa. Una aplicación de misión crítica no puede pararse. Las actualizaciones en los equipos que las soportan deben realizarse tomando medidas alternativas, como instalar servidores duplicados o redundantes que recojan temporalmente la carga de trabajo de los servidores sobre los que se va a actuar.

Vocabulario

Outsourcing o **externalización:** es el modo de contratación por el que un servicio concreto se contrata con una empresa externa especializada en ello.

2.2. El mantenimiento de la red

Cualquier cambio en la red es producto de la toma de una decisión. Siempre que algo cambia en un sistema, se debe a una razón que así lo aconseja.

Tomar decisiones siempre implica un riesgo: el del posible error en la decisión tomada. Sin embargo, frecuentemente, no se pueden retardar las decisiones, puesto que no tomarlas implicaría un problema mayor que el que se generaría si decidiéramos incorrectamente. El administrador de red tiene que tomar decisiones arriesgadas a menudo: no debe decidir imprudentemente, pero tiene que asumir el riesgo de la decisión con valentía.

La definición clásica de la virtud de la prudencia indica que es el hábito de elegir bien los medios para conseguir un buen fin. Aplicado a nuestro caso, revela la necesidad de conocer muy bien, no solo nuestra red, sino los productos de los proveedores y las tecnologías que incorporan. Sin este conocimiento será muy difícil que nuestra red se desarrolle correctamente a lo largo del tiempo.

Puede ser muy útil el análisis estadístico de las incidencias de la red. Por ejemplo, si observamos que un adaptador de red empieza a dar problemas, es mejor adquirir otro y sustituirlo enseguida con una parada programada que esperar a que se termine de estropear y genere una parada aleatoria que comenzará por buscar un proveedor que nos sirva un adaptador semejante al deteriorado.

La vigilancia del tráfico de red es otra de las actividades que ocuparán el tiempo del administrador. Debe conocerse qué volumen de tráfico, o lo que es lo mismo, qué cantidad de ancho de banda consumen las distintas aplicaciones.

Las actividades de mantenimiento más relevantes para el correcto funcionamiento de la red son aquellas que se relacionan con la seguridad. Vigilar la seguridad, afrontar las amenazas y atenuar los riesgos que atenazan a los sistemas de la red tiene que ser uno de los objetivos prioritarios del administrador que debe organizar esta seguridad mediante una defensa en profundidad.

CEO

SMR_RL_AAbad_08_PlanContingencias.docx

Documento que contiene información sobre un plan de contingencia ante desastres.

Ejemplos

Si en una compañía, el tráfico de red procedente del correo electrónico se ha multiplicado poderosamente en los últimos días, tenemos que pensar que podemos estar siendo invadidos por correo basura y habrá que instalar un antispam en nuestro sistema de entrada de correo.

2.3. Mejoras en la red, actualización y crecimiento

A la vista de lo que observamos que ocurre en la red y de la información que nos proporcionan los usuarios de los distintos servicios, el administrador tendrá que proponer las actuaciones que considere adecuadas para mejorar la calidad del servicio. En ocasiones, las actualizaciones no son requeridas por un problema o un cuello de botella en algún servicio, sino por el propio avance tecnológico.

Por ejemplo, supongamos que en un sistema que funciona correctamente necesitamos instalar una nueva aplicación. Al leer los requisitos de instalación de esta aplicación, nos damos cuenta de que requiere una versión del sistema operativo más actualizada de la que tenemos. Si queremos la aplicación, no habrá más remedio que actualizar el sistema operativo. Sin embargo, la actualización del sistema operativo implica que se requerirá más espacio en disco y puede aparecer un cuello de botella en el sistema por falta de espacio de almacenamiento. Esto requerirá que el administrador de la red mueva algunos servicios de disco a otro servidor.

Unas modificaciones en la red generan otras: la red es una entidad viva. En el mantenimiento ordinario de actualizaciones de los sistemas, hay que estar especialmente pendiente de los **parches** del sistema operativo, de las actualizaciones de los controladores y de las actualizaciones de las aplicaciones de usuario.

Muchos de los dispositivos de red tienen su propio sistema operativo integrado en sus memorias. Con frecuencia, los fabricantes publican actualizaciones para estos sistemas operativos que habrá que descargar y actualizar en las memorias flash de estos dispositivos. En estos casos, es muy importante seguir paso a paso las instrucciones del fabricante, pues estas operaciones son muy críticas y cualquier fallo en ellas suele implicar una avería irreparable del dispositivo.

Por último, habrá que revisar periódicamente el sistema de cableado que está más expuesto a averías, por ejemplo, el sistema de latiguillos del cableado horizontal en contacto con los **escritorios** de los usuarios.

Vocabulario

Parche: es una actualización que afecta a una parte de un sistema operativo y que corrige algún error, tapa algún agujero de seguridad, introduce alguna mejora o implementa una nueva funcionalidad.

Vocabulario

Escritorio: suele utilizarse este término para el conjunto de aplicaciones clientes que puede ejecutar el usuario desde su ordenador cliente.

2.4. Vigilancia y gestión de la red

Una vez instalada la red, y en pleno funcionamiento, se debe pasar al periodo de observación y medida con el fin de asegurarnos de que se obtiene el mayor rendimiento posible. Esta tarea se compone de una fase de análisis de la red con la elaboración de unas estadísticas sencillas que sirvan de apoyo para la proposición de medidas correctoras en los cuellos de botella que se produzcan o en la incorporación de mejoras.

A. Tráfico de red

Como ya hemos estudiado, algunas redes como Token Ring gestionan perfectamente las situaciones de tráfico intenso en la red. Sin embargo, otras como Ethernet, que son las que normalmente se utilizan, se comportan mal cuando están sobrecargadas. Esto hace importante la observación periódica del tráfico de red, así como de los parámetros por los que se regula; por ejemplo, en Ethernet, se podría medir el nivel de colisiones habidas frente al volumen de datos transferidos con éxito.

En el mercado existen aplicaciones que analizan el tráfico de red. A veces, incluso vienen incorporadas con el propio sistema operativo de red (Fig. 8.14). Los parámetros que suelen analizar son muy variados y dependen del tipo de protocolo utilizado y del tipo de red, así como de la topología de la misma.

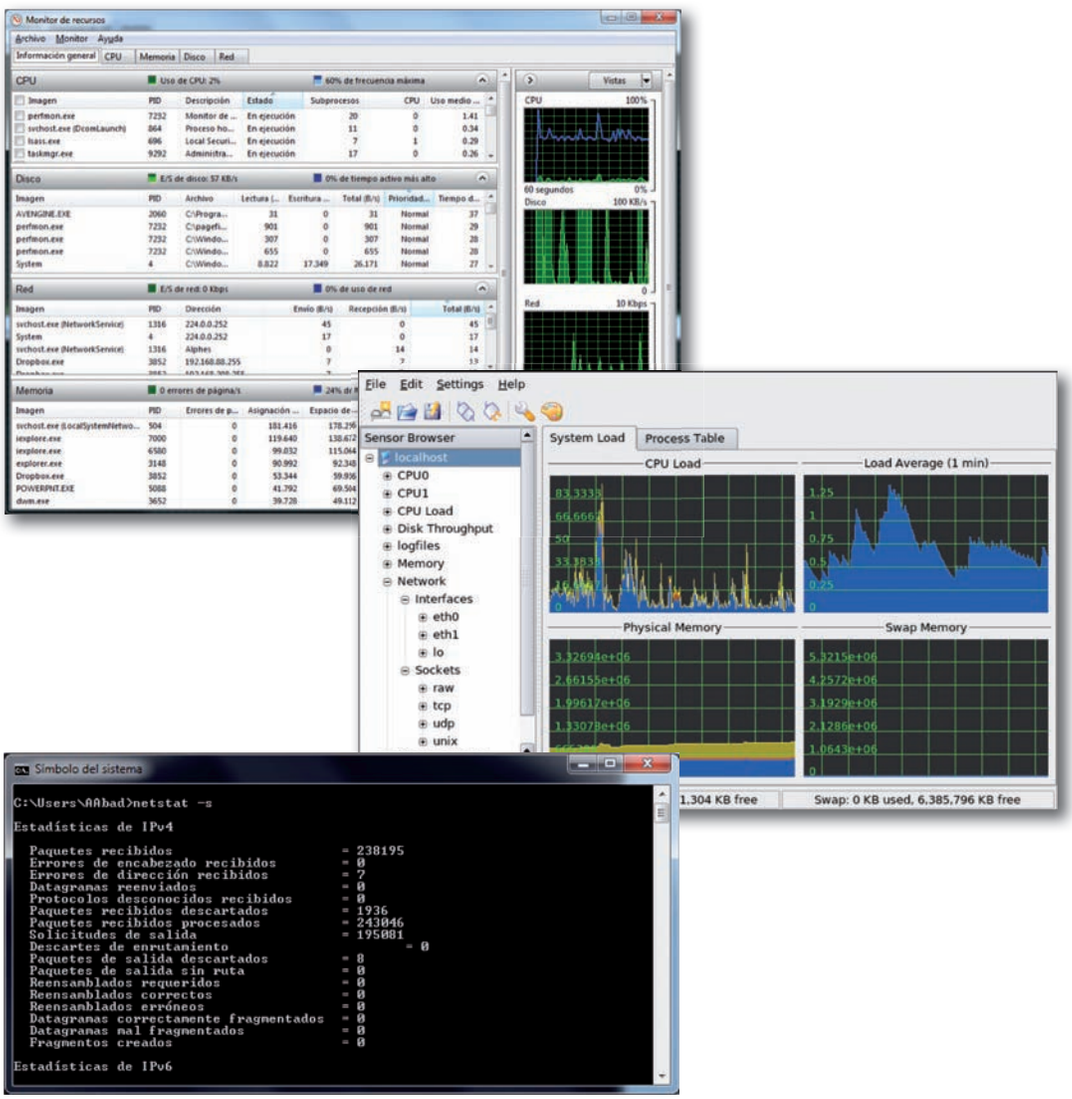


Fig. 8.14. *Monitor de recursos en Windows, a la izquierda; la versión Linux, a la derecha. Abajo, ejecución de «netstat –s» que proporciona información estadística de la red.*

Vocabulario

Analizador de red o *sniffer:* es un escuchador de la red que espía todo el tráfico que pasa por el segmento de red en que se instala con objeto de analizar lo que circula por la red.

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

Posibles soluciones de mejora para estos problemas podrían ser la asignación de máscaras de red más ajustadas a las necesidades de la propia red, modificaciones en la topología de red, concentrar los nodos que generan mucho tráfico en segmentos de red rápidos, asegurarse de que se cumplen las especificaciones de los fabricantes en cuanto a longitudes de cables y parámetros eléctricos, etc. También es posible segmentar la red con la utilización de *switches* y encaminadores, confeccionando redes conmutadas y encaminadas.

Ampliación

Monitorización de los protocolos de red

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

Esto es especialmente importante cuando los paquetes generados por algunos protocolos deben ser transportados a otra red a través de encaminadores, ya que estas máquinas trabajan con paquetes de protocolos previamente seleccionados. Cuando se dan situaciones de este tipo, es necesario observar frecuentemente el estado de puentes, encaminadores y pasarelas, puesto que un cuello de botella en alguno de estos elementos puede perjudicar la marcha global de la red, aunque en ella no haya un tráfico intenso: la velocidad del tráfico se regula siempre por el flujo del punto más lento.

Claves y consejos

Si el tráfico de red es muy intenso, no habrá más remedio que dar un salto tecnológico en la composición de la red. La evolución natural de una red Ethernet es pasar a Fast Ethernet y de esta a Gigabit Ethernet. También se pueden construir segmentos de fibra óptica o configurar parte de la red con ATM.

B. Planes de auditoría

La auditoría es una de las funciones más importantes de los administradores de las redes. En las grandes corporaciones, la seguridad de los sistemas y de la red depende de un departamento especializado, pero lo habitual es que los administradores ordinarios de la red se ocupen también de la seguridad de sus sistemas.

Para que un sistema de auditorías funcione correctamente tiene que cumplir varios requisitos. En primer lugar, el sistema de recogida de datos tiene que ser hábilmente diseñado para que, sin inundarnos de información, sea capaz de recoger los datos necesarios para detectar averías o intrusos.

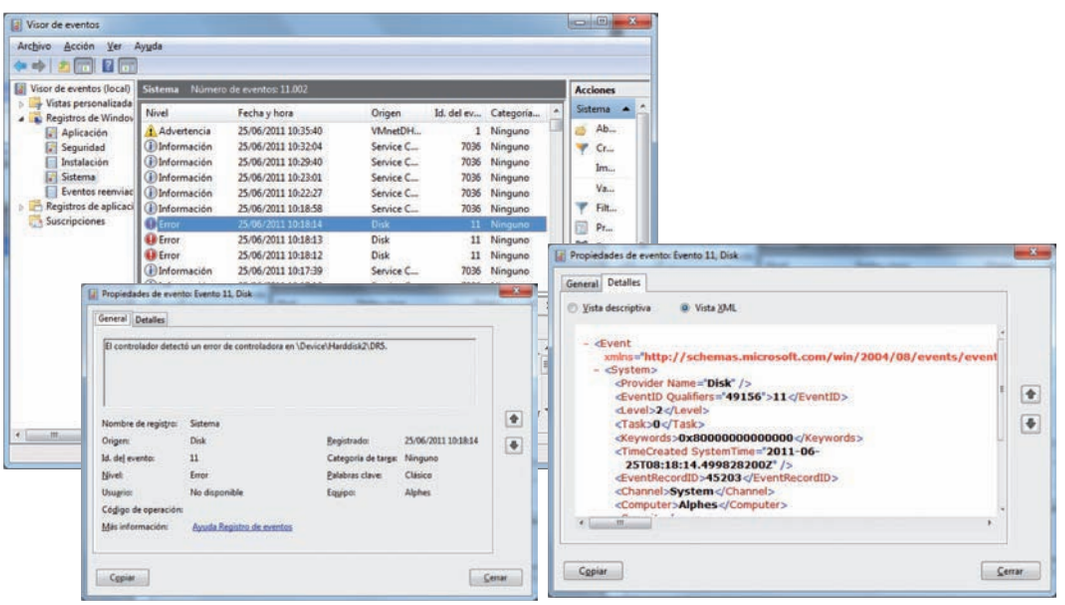


Fig. 8.15. *Visor de sucesos de Windows en su registro de sistema. Se ha elegido un evento que delata un error para averiguar más sobre el problema. Abajo, descripción del error en formato XML.*

Como vemos en la Fig. 8.15, Windows almacena la información de eventos de seguridad de modo que después puede ser visualizada y analizada desde una consola de administración. Desde allí podemos configurar el volumen de información que deseamos recoger, así como vaciar el almacén de eventos.

En segundo lugar, esta información recogida no servirá para nada si posteriormente no se analiza exhaustivamente. Debido al gran volumen de información que se suele generar, los administradores de grandes redes instalan aplicaciones especializadas en la detección de situaciones conflictivas a partir de las alarmas generadas, y esto no solo en un sistema, sino en toda la red.

Vocabulario

Falsos positivos: muchas veces las alarmas registradas en el sistema proceden de situaciones que no son de riesgo; es lo que se llama falsos positivos, pero en principio hay que analizarlas todas.

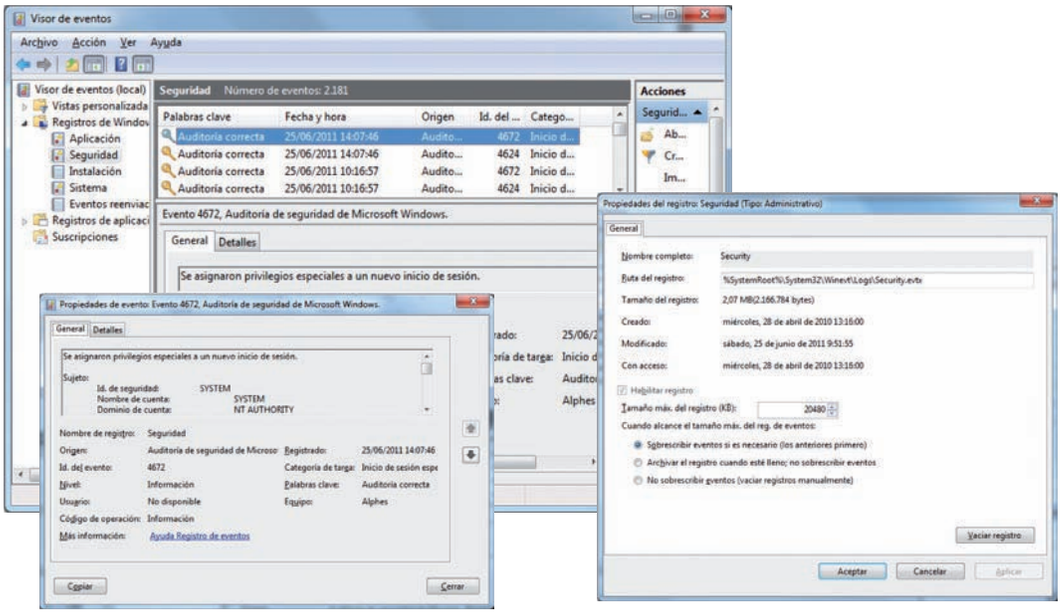


Fig. 8.16. *Visor de sucesos de Windows en su registro de seguridad (arriba). Abajo, a la izquierda, vista de uno de los sucesos de seguridad. Abajo, a la derecha, configuración del registro de seguridad.*

CEO

S M R _ R L _ A A b a d _ 0 8 _ ProtocolosGestion.docx

Documento que contiene información sobre:

1. Protocolos para la gestión de redes.
2. Analizadores de protocolos.

La seguridad de la red exige que todas las operaciones de auditoría y posterior análisis se integren dentro de un plan de acción en el que se especifique qué hacer en caso de que ocurra un determinado acontecimiento, sin olvidarse de las tareas periódicas que hay que realizar, incluso aunque los sistemas de detección no estén en situación de alarma.

Por ejemplo, diariamente hay que vigilar los registros del sistema, comprobar que los antivirus se han actualizado, detectar los intentos fallidos de conexión, etc.

Investigación

En la dirección **http://www.lavalys.com/** puedes descargar una versión de prueba de AIDA64 (anteriormente denominado Everest), una de las aplicaciones ampliamente utilizadas para monitorizar un sistema en red. Descárgalo, instálalo en un equipo en red y prueba su funcionalidad con objeto de que te acostumbres a trabajar con este tipo de aplicaciones.

Una buena aplicación libre para la monitorización de la red es ntop, que corre tanto en Windows como en Linux. Puede descargarse de **http://www.ntop.org**

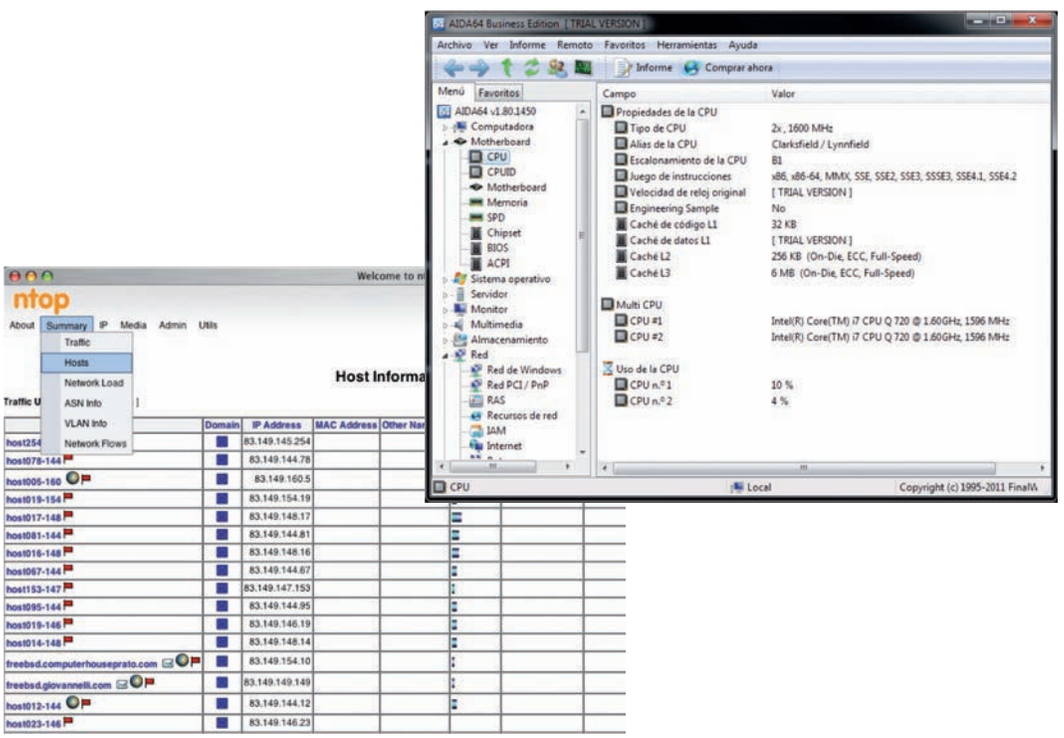


Fig. 8.17. *Arriba, vista de la información sobre CPU desde AIDA64 para un sistema sobre Windows. Abajo, página web de ntop sobre Linux para la visualización del tráfico de la red.*

C. Consolas de gestión remota

Fundamentalmente, hay dos modelos de gestores remotos: los que se encargan de la gestión de equipos y los que tienen por función la gestión de consolas. El número de elementos en una red que se puede gestionar es tan grande que es imposible abarcarlo todo.

Un **gestor de consolas,** de sesiones remotas o simplemente gestor de control remoto, es una aplicación que es capaz de visualizar sobre una consola local lo que está ocurriendo en una consola remota. Los más avanzados son capaces también de crear verdaderas sesiones remotas, no solo simularlas. Además, los gestores más avanzados son capaces de ejecutar acciones en el sistema remoto comandados desde el sistema local.

Las consolas de sesiones remotas tienen dos componentes, un cliente y un servidor, que crean sesiones remotas desde la estación cliente hasta la estación servidora. Algo parecido a lo que hace Telnet pero gráficamente y con más valor añadido.

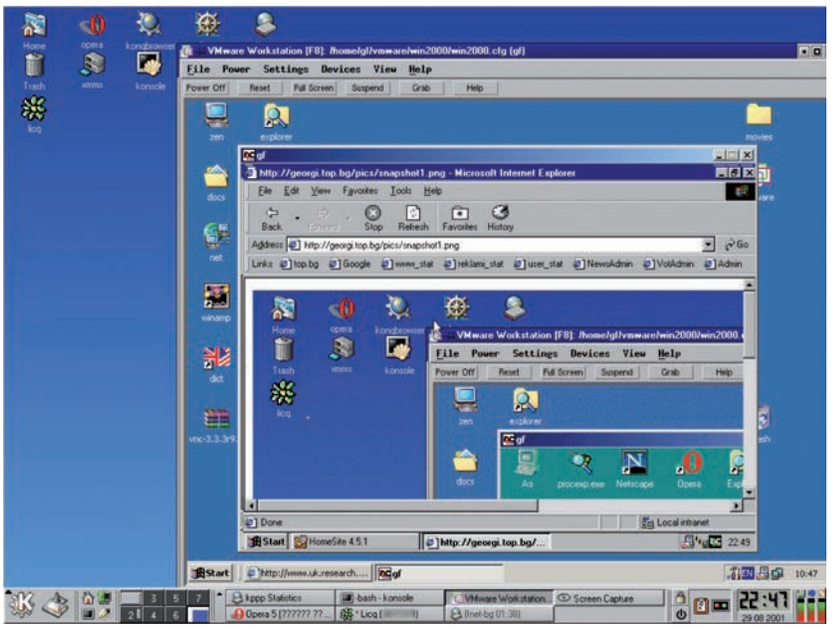


Fig. 8.18. *Secuencia de acceso virtual mediante gestores de consolas sobre diferentes sistemas.*

Destacamos la solución VNC por ser *freeware* y de amplio uso (se puede descargar desde **www.realvnc.com**) y además está soportado por muchos sistemas operativos: UNIX, Linux, Windows en todas sus variantes, OS/2, BeOS, MacOS, PalmOS, etc. La mayor parte de las distribuciones Linux, bajo diferentes nombres, incorporan VNC de serie.

La consola de VNC (que hace de cliente) conecta con un agente que hace de servidor y que se instala en el ordenador de destino de la conexión. En la Fig. 8.18 se puede ver de afuera hacia dentro un sistema Linux (con escritorio KDE), que tiene virtualizado mediante VMware un sistema Windows, que a su vez se conecta mediante un cliente VNC integrado en Internet Explorer al servidor VNC de otro sistema Linux, que a su vez visualiza otra estación Windows virtualizada sobre VMware que tiene abierta otra sesión VNC. Como se ve, como las consolas pueden invocarse o contenerse unas a otras, las posibilidades son inmensas.

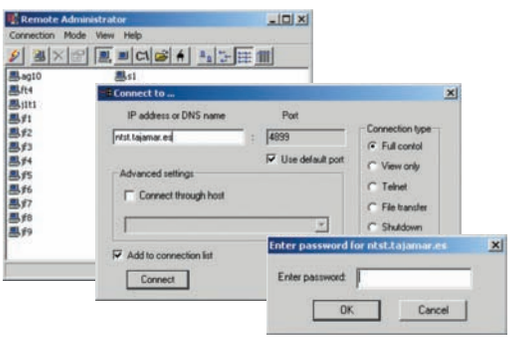


Fig. 8.19. *Secuencia de conexión de la consola de Remote Administrator.*

Remote Administrator es otra de las consolas remotas más utilizadas, aunque no es gratuito. Tiene algunas posibilidades más que VNC, pero el modo de instalación y de gestión de consolas es muy parecido.

En la Fig. 8.19 podemos ver la consola de gestión de Remote Administrator (cliente de conexión). Se abre una conexión contra un ordenador, en donde elegimos el puerto por el que se ha instalado en el destino el agente de escucha (la parte de servidor de VNC), que, por defecto, es el puerto 4899, aunque puede cambiarse. Una vez que intentamos la conexión, el agente servidor nos pedirá que nos identifiquemos para lograr una conexión remota que captura los eventos de pantalla, ratón y teclado.

En sistemas Windows, tanto de cliente como de servidor, también se pueden crear conexiones remotas a través de la gestión remota del escritorio. El protocolo de comunicaciones utilizado por el escritorio remoto de Microsoft es **RDP** *(Remote Desktop Protocol).* Los nombres formales que utilizan las aplicaciones RDP para efectuar sus conexiones varían dependiendo de las versiones de Windows, pero son semejantes a *Conexión a escritorio remoto, Cliente de Terminal Server* o *Servicios de terminal.*

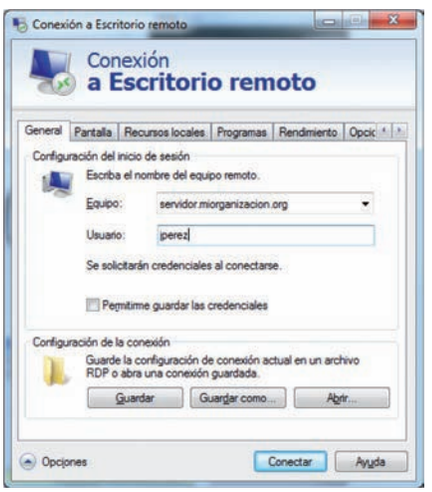


Fig. 8.20. *Cliente de conexión a escritorio remoto desde Windows 7.*

Los clientes RDP válidamente licenciados se podrán conectar al escritorio del servidor RDP virtualizándole. Estos clientes pueden ser tanto Windows como Linux o cualquier otro sistema operativo para el que se haya implementado el protocolo RDP.

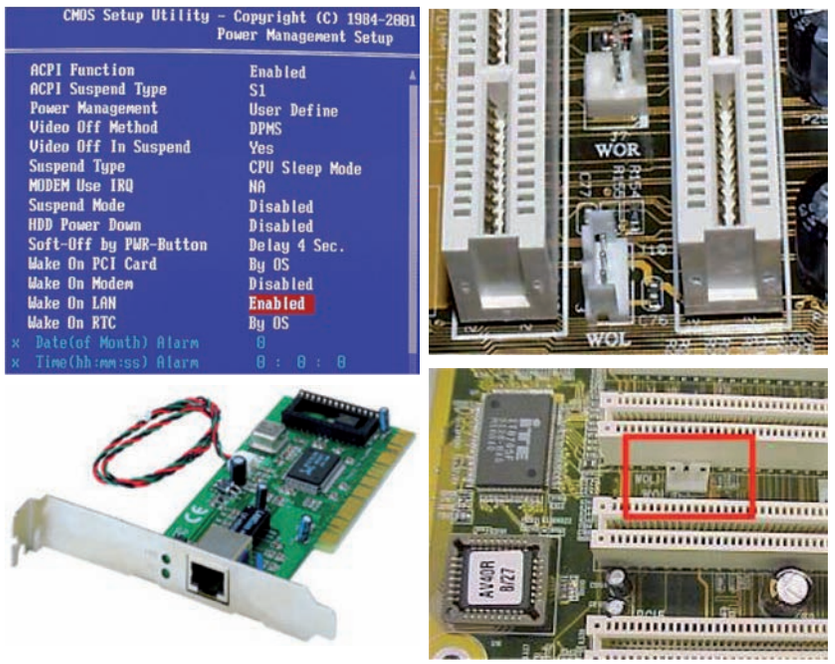


Fig. 8.21. *Detalle de la BIOS, tarjeta de red y placa madre compatibles con WOL.*

D. Despertar un sistema desde la red

Arrancar o parar un sistema no es una operación muy costosa en tiempo; sin embargo, exige desplazarse a la ubicación física del equipo para manipular el botón de encendido o hacer una parada del sistema por software. Algunas tecnologías informáticas permiten que estas operaciones se puedan realizar remotamente, sin necesidad de estos desplazamientos.

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

La gestión previa al inicio de WfM está enfocada a la gestión de estaciones de trabajo cuando estas están apagadas. La tecnología **PXE** (*Previous eXecution Environment,* entorno de ejecución previo al inicio), especificación para la gestión en adaptadores de red, es obligatoria bajo WfM: tanto la BIOS del PC como la tarjeta de red deben soportarlo. Con la tecnología PXE, la tarjeta de red permanece siempre a la escucha de la red, aun con el PC apagado, de modo que a una orden concreta del servidor, la tarjeta ordena encenderse al PC arrancando el software de sistema: una tecnología denominada **WOL** *(Wake On LAN).*

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

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

Tecnología *Wake on LAN*

WOL o Wake on LAN es una tecnología que permite despertar a un equipo cuando recibe por la tarjeta de red, que permanece siempre a la escucha aun con el equipo apagado (que no desconectado de la red eléctrica), una trama específica denominada trama mágica o *magic packet* desde un gestor de arranque. Como esta característica opera en el nivel de enlace (capa 2 de OSI), el encendido solo funcionará dentro del mismo segmento de la red de área local. Si se quieren despertar máquinas remotas, hay que utilizar mecanismos de enrutamiento junto con WOL.

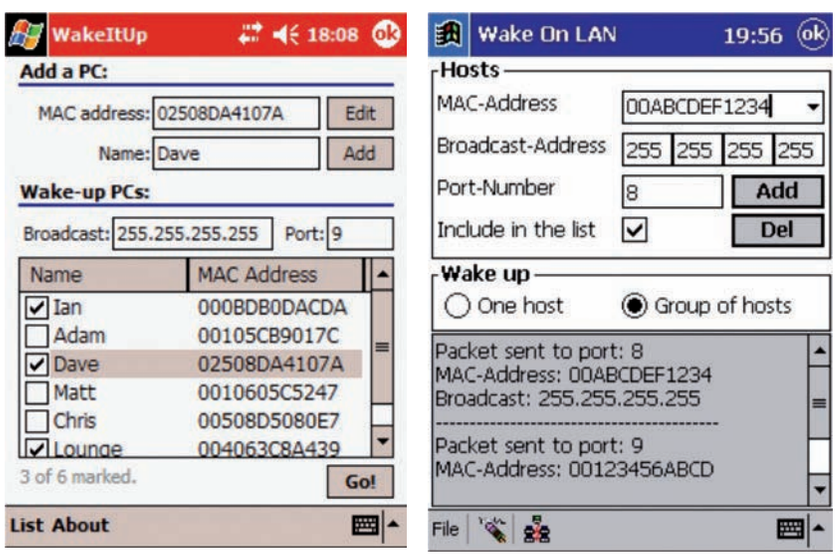


Fig. 8.22. *Capturas desde un pocket-PC de una aplicación WOL.*

Obviamente, no todos los adaptadores de red son compatibles con estas tecnologías. Si se desea disponer de esta función hay que asegurarse de que el hardware del sistema es compatible con WOL. Esto implica que las BIOS del PC tienen que soportar esta tecnología, que la placa madre tenga el conector WOL que conecte la tarjeta de red con la placa madre y que este adaptador de red también sea compatible con WOL. El adaptador de red deberá incluir un cable de conexión entre la tarjeta y la placa madre a través del cual la tarjeta de red despertará al sistema.

Esta tecnología es muy interesante porque nos permitirá arrancar los equipos de un modo muy sencillo, sin necesidad de desplazarnos. Incluso podremos utilizar tecnologías inalámbricas para ordenar el arranque desde dispositivos de mano como un pocket-PC.

3. Incidencias, soporte y legalidad

Cuando algo en una red deja de funcionar, hay que actuar lo más rápidamente posible. Pero, en concreto, ¿qué es lo que hay que hacer? La respuesta a esta pregunta tan importante para el administrador depende del diagnóstico de la avería.

Las averías más frecuentes son fáciles de diagnosticar, porque tienen efectos que solo pueden ser producidos por causas bien determinadas, de modo que, conociendo el efecto negativo producido, somos capaces de determinar su causa y actuar sobre ella. Sin embargo, ocasionalmente hay averías que son muy difíciles de diagnosticar, en donde no se sabe si la causa de la avería viene de un mal funcionamiento del hardware, del software o de la red.

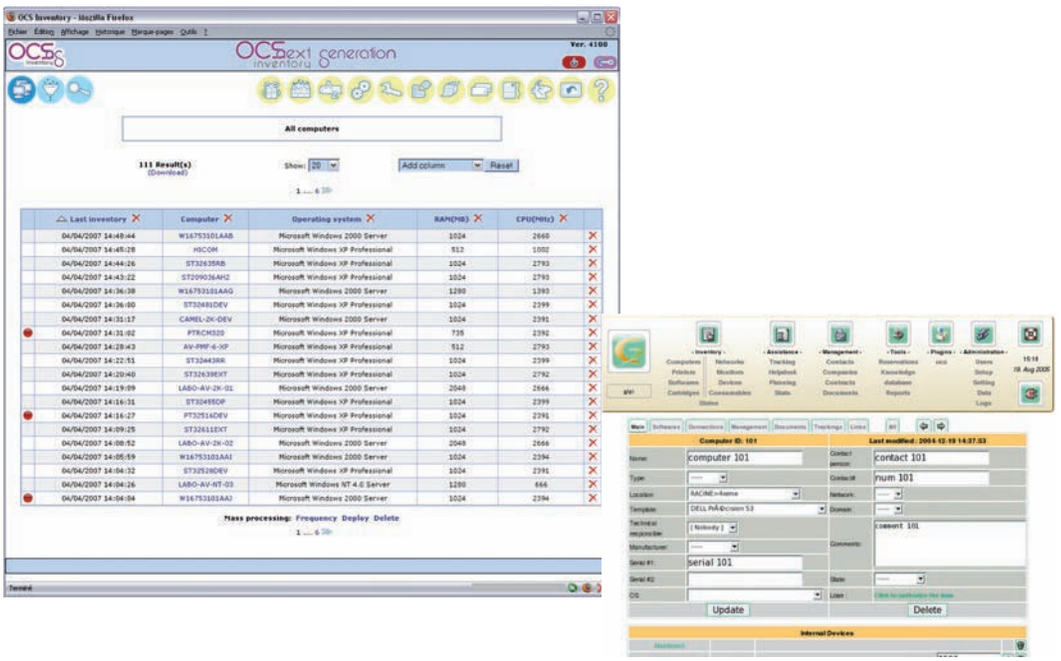


Fig. 8.23. *A la izquierda, vista de OCS, que es un gestor de inventario de hardware y software. A la derecha, vista de GLPI, un gestor de incidencias que puede colaborar con OCS. Ambos son aplicaciones de código libre y sus consolas son de tipo web.*

Esto ocurre especialmente si el efecto no deseado que produce la avería puede ser originado por varias causas distintas. Por ejemplo, que no funcione un ratón puede ser porque el ratón se haya deteriorado, porque lo que se haya estropeado sea el puerto del ratón, porque el controlador del ratón se haya corrompido, porque tenemos un virus que actúa sobre el ratón moviéndolo sin nuestra intervención, etc.

La gravedad de la avería se mide por el daño que realiza, que básicamente se evalúa mediante tres factores:

- El coste de tener parado el sistema en que se produce la avería, que obviamente deja de producir durante el tiempo de avería más el tiempo de reparación.
- El tiempo que se requiere para realizar la operación de reparación.
- El coste de reparación.

Después de un correcto diagnóstico, hay que averiguar el procedimiento que permite solucionar la avería. Efectivamente, de nada serviría conocer el diagnóstico si no conocemos la terapéutica. Aquí entra de lleno la preparación técnica de los administradores de la red.

Por último, hay que considerar que el objetivo final de cualquier acción en contra de una avería es el restablecimiento del servicio lo antes posible, por lo que el tiempo es siempre un factor crítico.

Claves y consejos

Tener diagnosticada una avería significa haber hallado las respuestas correctas a unas cuantas preguntas. Aquí hemos seleccionado las siguientes:

Localización: ¿dónde se ha producido la avería? Implica conocer en qué ordenador o en qué cable se encuentra, la ubicación física en el edificio, etc.

Causa de la avería: ¿qué produjo la avería? Por ejemplo, hubo una subida de tensión eléctrica, alguien dañó un cable, se produjo una inundación, atacó un virus, etcétera.

Repercusión: ¿qué daños ha causado la avería? Puede provocar que un sistema no arranque, que se pierda información, que se pare una unidad de negocio, etc.

Ejemplos

La rotura de una tarjeta de red en un servidor se puede considerar una avería muy grave porque paraliza totalmente que los usuarios puedan servirse de él, ya que lo hacen a través de la red, que es precisamente lo que no funciona. Sin embargo, el tiempo de reparación es muy breve, porque sustituir una tarjeta de red es algo sencillo y rápido. El coste de reparación también será muy bajo, por lo que concluimos que esta avería de tan gran impacto en un servidor no es tan grave como parecía en un principio.

Otra cosa distinta sería si la tarjeta de red del servidor es muy especial, no tenemos repuesto de ella y es difícil encontrarla en el mercado. Este es un ejemplo de cómo una circunstancia externa a la propia avería la agrava significativamente.

CEO

SMR_RedesLocales_08_InstalaGLPI.pptx

Documento que contiene realizaciones prácticas sobre la instalación de GLPI sobre Ubuntu.

CEO

SMR_RL_AAbad_08_DocumentacionTecnica.docx

Documento que contiene información sobre:

1. Documentación sobre diagnóstico de averías.
2. Fuentes de información técnica y certificación profesional.

CEO

SMR_RL_AAbad_08_GestionIncidencias.docx

Documento que contiene información sobre:

1. Cuellos de botella y necesidades futuras de la red.
2. Presupuestos y calendario de actividades.
3. Gestión del proyecto de cambio.

3.1. Gestión de incidencias

En los procedimientos empresariales siempre se acaba intentando dar soluciones inteligentes a los problemas que se plantean. Realmente esto es lo que busca una empresa cuando contrata a un empleado. Luego, de modo secundario, el empleado necesitará unas herramientas técnicas para poder desarrollar eficazmente su trabajo.

Para enfrentarse a los problemas, actuales o en el futuro inmediato, caben dos posibilidades: gestión **reactiva** o gestión **proactiva.**

En el caso de la gestión reactiva, se trata de proporcionar soluciones a los problemas planteados en función de cómo se generen o cómo se planteen. Así, si un adaptador de red se estropea hay que cambiarlo inmediatamente. La solución se propone como una reacción al problema.

En la Fig. 8.24-B se puede ver que la experiencia técnica solo se alcanza al finalizar la gestión de la incidencia, ya que la pauta de actuación está regida por las incidencias que vayan surgiendo.

Sin embargo, con la gestión proactiva no esperamos a que se produzca el problema para reaccionar: antes de que el problema se radicalice se establecen medidas que lo palien o lo atenúen. En el caso de nuestro adaptador de red, cuando el administrador detecte que la interfaz empieza a dar errores con mayor frecuencia de lo que viene siendo habitual, podemos programar su sustitución.

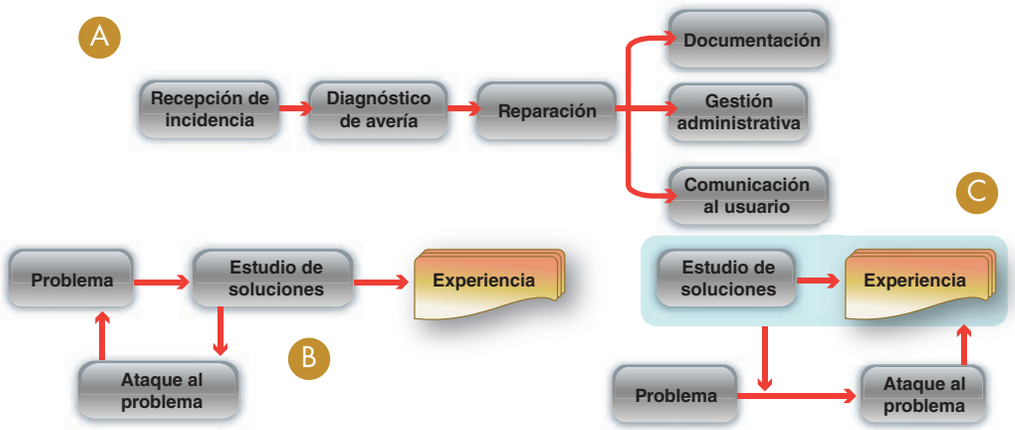


Fig. 8.24. *A) Diagrama esquemático de la gestión de una incidencia. B) Actuación reactiva. C) Actuación proactiva.*

Actividades

5. Descarga de Internet la aplicación VNC e instálala en varios equipos de la red, a ser posible sobre distintos sistemas operativos para los que existe la versión de VNC.

Ahora extrae el cliente VNC y cópialo en el disco de alguna estación de la red. La herramienta de cliente no requiere instalación. Seguidamente prueba a realizar conexiones desde el cliente contra los equipos en donde hayas instalado el servidor VNC. Ensaya distintas soluciones de conectividad.

Ten en cuenta que como estas aplicaciones de gestión remota, como VNC, dejan puertas traseras de conexión, algunos antivirus las clasifican como *malware*. Si el antivirus que tienes instalado en la máquina de pruebas declara VNC como un ataque al sistema, deberás configurar el antivirus para declarar inocuo a VNC, o deshabilitar el antivirus durante las pruebas, aunque esto último no es aconsejable.

6. Repite el ejercicio anterior realizado con VNC utilizando ahora Remote Administrador. Aunque esta utilidad no es gratuita, se puede conseguir una versión de evaluación por unos días en la web y puedes utilizarla para la realización del ejercicio.

7. Estudia las páginas **http://www.elguille.info/sistema/escritorioremoto.htm** y **http://www.ujaen.es/sci/redes/vpn/esc_remoto.html** para aprender a realizar conexiones de escritorio remoto.

Posteriormente, en el laboratorio, sobre dos sistemas Windows, configura una conexión remota desde una de las estaciones a otra.

Ten en cuenta que las versiones Home de Microsoft Windows tienen el cliente RDP (pueden efectuar conexiones), pero no disponen del servidor RDP (no pueden aceptar conexiones desde otros nodos).

3.2. La función de soporte

Los usuarios de una red son de la máxima importancia, ya que son quienes utilizan los servicios que provee. Por tanto, una buena atención a los usuarios redundará en una mayor eficacia de la red incluso en las mismas condiciones técnicas.

Además, los usuarios de una red son una fuente importante de información sobre lo que pasa en ella. Muchas veces serán ellos los que nos proporcionen pistas sobre los cuellos de botella que experimentan. Otras veces, sugerirán procedimientos que les faciliten el trabajo y, con ellos, nos darán nuevas ideas para planificar el crecimiento de los recursos tecnológicos.

Sin embargo, no todo lo que pide un usuario de la red puede proporcionársele. La razón estriba en que cuando el personal no técnico solicita algún servicio no suele tener conciencia del coste, de la complejidad o de los efectos laterales indeseados que lleva consigo. En estos casos, el administrador de red junto con los responsables económicos, si fuera el caso, deben considerar la propuesta y decidir sobre ella.

Para que esto no se tenga que hacer así en todas y cada una de las peticiones de los usuarios, conviene distinguir lo que es soporte habitual a los usuarios de lo que sería un soporte extraordinario que requeriría una consulta especial.

El departamento de soporte debe tener claro cuáles son las actuaciones de soporte ordinarias que son capaces de llevar a cabo y los procedimientos a seguir en caso de una solicitud de soporte extraordinario. Esta información debe ser hecha pública para que sea conocida por todos los usuarios de la red y aprendan a pedir lo que sea necesario para ellos en los departamentos adecuados.

Para poder proporcionar su servicio, el departamento de soporte debe utilizar herramientas de gestión de consolas remotas como las que ya se han visto: VNC, conexión a escritorio remoto, etc.

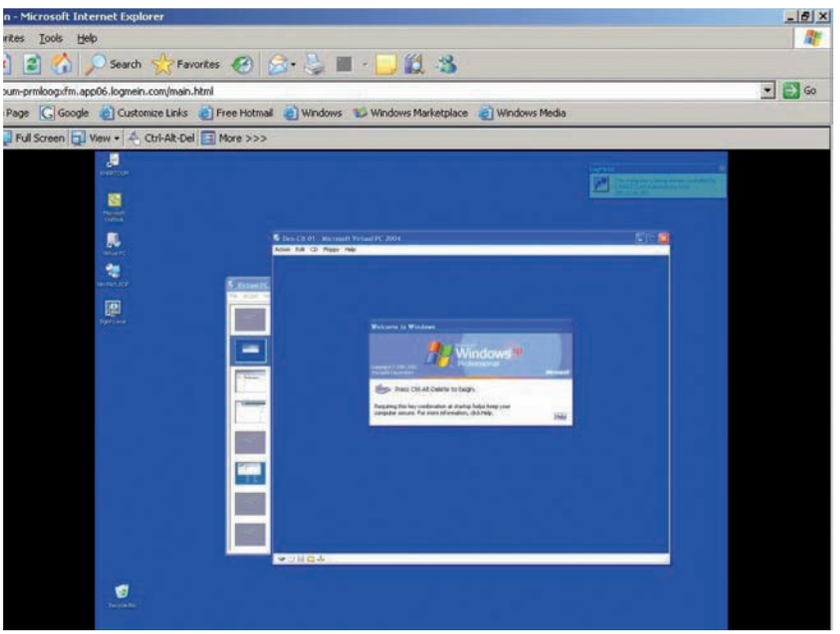


Fig. 8.25. *Vista de Logmein en su versión gratuita, aplicación muy útil en los servicios de help desk que gestiona conexiones remotas.*

Estas herramientas presentan problemas cuando tienen que atravesar cortafuegos ya que se basan en conexiones punto a punto que frecuentemente son filtradas por los *firewalls,* especialmente si utilizan NAT en la frontera entre la LAN e Internet.

Para solucionar esto se dispone de software, patrocinado por empresas de servicios, que gestionan las conexiones remotas sobre protocolo HTTP o HTTPS, capaces de atravesar cualquier cortafuegos que permita la navegación sobre Internet.

Algunas de estas aplicaciones son Logmein, NTF o Netviewer; aunque hay muchas más disponibles.

Claves y consejos

Los usuarios frecuentemente son una fuente de información muy importante, aunque no siempre nítida. Es una buena práctica profesional tener una actitud de escucha constante hacia lo que los usuarios de la red pueden aportar o sugerir sobre ella.

Ejemplos

El departamento de soporte o *help desk* puede determinar que se puede dar soporte de una suite de herramientas ofimáticas, de la configuración del perfil de los usuarios en el sistema operativo y de localización de los servicios de red. Además, este departamento recogerá todas las incidencias de averías, que pasará al departamento técnico encargado del mantenimiento.

Según esto, constituirían actuaciones extraordinarias de soporte la petición de instalación de una aplicación no prevista en el sistema, la creación de un buzón de correo extraordinario, un cambio de sistema de cableado para poder conectar otro equipo, etc.

Vocabulario

***Outsourcing* o externalización:** las grandes empresas suelen tener un departamento especializado en el soporte de los usuarios, pero en las pequeñas compañías, suele ser el departamento de informática el que se encarga también de proporcionar soporte a los usuarios de la red. Existe una tendencia actual a externalizar (así es como se llama en la jerga empresarial) el soporte a los usuarios mediante la contratación a otras empresas para que lo hagan en su nombre: se trata de un nuevo servicio de *outsourcing*.

CEO

SMR_RL_AAbad_08_SoporteUsuarios.docx

Documento que contiene información sobre comunicación de soporte con el usuario.

3.3. Legalidad y ética en las TIC

Internet es la gran herramienta de trabajo por excelencia para el administrador de red puesto que se convierte en su mayor fuente de información y de recursos disponibles, además del canal de comunicación imprescindible para su relación con otros administradores con los que comparte mucha información y experiencia profesional.

Los usuarios de la red son personas, e Internet está modificando sus hábitos. Esto ha llevado a la sociedad a plantearse las ventajas e inconvenientes que produce la aplicación de las nuevas Tecnologías de la Información y de la Comunicación (TIC) al entorno humano.

A. Internet y delincuencia

A pesar del convencimiento generalizado de las grandes ventajas que aporta Internet o, en general, los servicios de telecomunicación, no todo en Internet es maravilloso. Gran parte de los accesos a los servicios que provee Internet no necesitan ninguna identificación de los usuarios, lo que ha generado un incremento de las actividades delictivas, sirviéndose de la red como medio, potenciadas por el anonimato en que se escudan los infractores de las leyes.

El principal problema consiste en que no hay un modo claro de controlar la información que viaja por Internet, puesto que la red está en manos de multitud de pequeños y grandes propietarios, y esto dificulta llegar a acuerdos globales en materia de seguridad o de lucha contra la delincuencia o la violación de derechos de autor.

Evidentemente, la utilización moral o inmoral de Internet depende de cada usuario de la red. El ser humano está dotado de una naturaleza libre, y depende de este el uso, bueno o malo, que haga de las herramientas de las que dispone. Aun así, se requiere que los poderes legislativos, tanto nacionales como internacionales, regulen las actividades de comunicación humanas mediante leyes justas, sin perjuicio del respeto por otros derechos directamente relacionados, y en concreto por el derecho a la información.

B. Software legal y protección de datos personales

Todo software debe llevar una licencia asociada. Salvo en el caso del software libre que, en la mayor parte de los casos, se distribuye gratuitamente, el resto de los programas deben instalarse previa adquisición de una licencia de pago al distribuidor o fabricante de software.

Para asegurarse de esto, muchas aplicaciones incorporan protecciones que impiden su copia, instalación o ejecución. Frecuentemente, estas protecciones son violentadas con técnicas de ingeniería inversa, pero, aunque por este procedimiento las aplicaciones se dejaran instalar y ejecutar, esto no hace legal la situación de nuestro software. La piratería de software es un delito castigado administrativa y penalmente.

El administrador tiene entre sus misiones garantizar que todo el software que se instala en la red es legal, es decir, que se ha adquirido una licencia de software por cada copia instalada. A veces se pueden instalar más copias que el número de licencias adquiridas: el contrato de licencia de software que aceptamos al realizar la instalación de la aplicación nos precisará cómo funcionan las licencias de esa aplicación.

Ampliación

Internet es un ejemplo obvio en donde se observa claramente la diferencia entre ilegalidad e inmoralidad. Una actividad puede ser delictiva (ilegalidad) en un país y no en otro. Los usuarios de este primer país podrán acceder a un servicio ilegal, aunque perfectamente lícito en el país que proporciona el servicio. Sin embargo, algo parece claro: la inmoralidad procede no de la prohibición que emana de las leyes de un país, sino del daño que ciertas actividades producen en las personas o en sus legítimos intereses, con independencia de que estén recogidas o no en un ordenamiento jurídico.

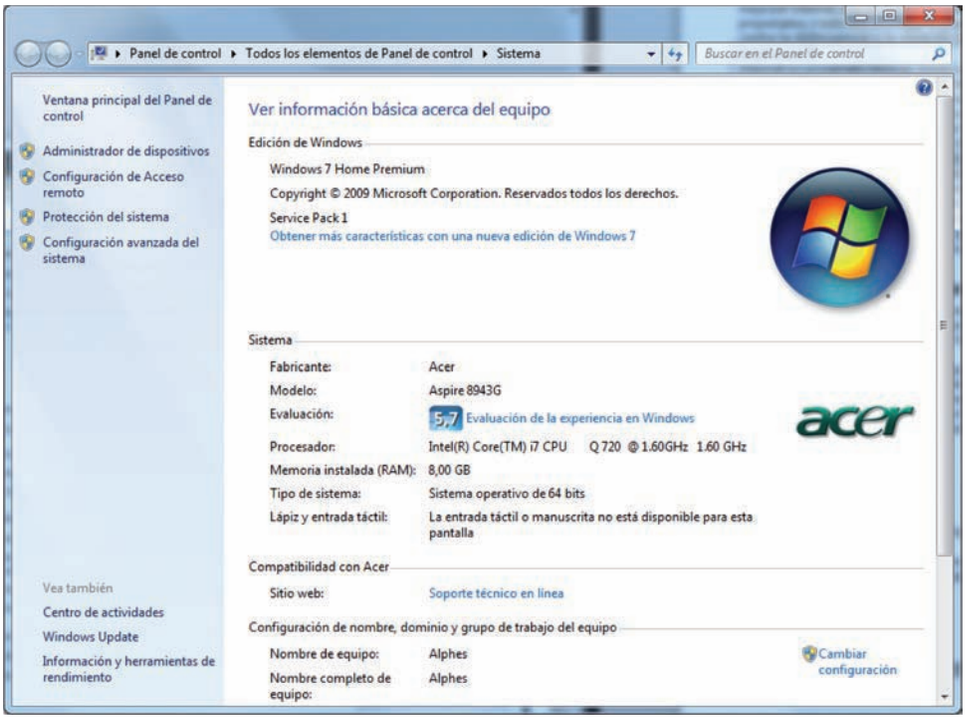


Fig. 8.26. *Logotipo de software original para un sistema Windows 7.*

Del mismo modo que los sistemas deben tener legalizado su software, el administrador también tiene que prever la protección de los datos personales a la que obligan las leyes. Las administraciones públicas exigen que las bases de datos o ficheros que contengan información sobre personas deban estar especialmente custodiadas. Además, estas bases de datos deben estar registradas en los registros institucionales previstos por las leyes de protección de datos. También hay que habilitar los mecanismos apropiados para que las personas cuyos datos custodiamos puedan ver, modificar o anular la información sobre ellas.

Actividades

8. Declara si las actuaciones siguientes en la gestión de una avería son o no correctas:

a) Una tarjeta de red ha empezado a fallar, pero no la sustituimos hasta que no se estropee totalmente.

b) Un virus ha dañado un sistema operativo. Nos encontramos con el administrador en un pasillo y se lo comunicamos de viva voz.

c) El servicio de *help desk* repara una avería de un usuario, pero no le comunica que la reparación ya ha sido realizada.

9. Descubre cuáles pueden ser los efectos laterales contraproducentes en la siguiente actuación profesional:

Cuando encendemos un PC nos indica que la dirección IP está duplicada en la red. Para evitar la colisión cambiamos la dirección IP local por otra, a pesar de que la que había originalmente era la correcta.

10. Desde la dirección **https://secure.logmein.com/ES/** puedes descargar Logmein en su versión gratuita. Instálala en una estación Windows y prueba su funcionamiento para conectarte a otros sistemas simulando una actuación de soporte *help desk*.

Investigación

En la dirección **http://www.navegacionsegura.es** tienes algunos consejos para aprender a navegar de manera responsable y evitando riesgos inútiles. Lee el documento y asegúrate de que comprendes bien en qué consisten estos riesgos para tratar siempre de evitarlos.

Ampliación

La BSA *(Business Software Alliance)* es una organización sin ánimo de lucro que se encarga de concienciar a los usuarios de la necesidad de software legal, además de perseguir la piratería informática. Se puede conseguir más información sobre la BSA en su sede web: **http://www.bsa.org**

4. Documentación de la red

Ante la posibilidad de cualquier problema, cambio o mejora en la red, es conveniente tener documentado correctamente el sistema con la información sobre él lo más actualizada posible. Cada administrador de red elige las técnicas de documentación que considere oportunas. No obstante, los documentos que no pueden faltar son los siguientes:

- **Mapa de red.** Es la representación gráfica de la topología de la red, incluyendo tanto conexiones internas como externas. Esta documentación puede apoyarse en un plano del edificio en donde se instala la red. Suelen confeccionarse dos tipos de mapas de red: lógicos y físicos. En los lógicos (también denominados funcionales) se indica la funcionalidad del elemento que se describe así como sus direcciones, papel que desempeña, etc. En el caso del mapa físico, interesa sobre todo la especificación de la conectividad del cableado.
- **Mapa de nodos.** Se compone de una descripción del hardware y del software que se instala en cada nodo, así como los parámetros de su configuración, modelos, marcas, direcciones de red, etc. La documentación debe permitir la creación de un histórico de cada nodo que registre la evolución de sus averías, actualizaciones de software, etc.
- **Mapa de protocolos.** Es la descripción de la organización lógica de la red, así como de los protocolos utilizados globalmente, por ejemplo, las direcciones de máscaras de red, configuración de las pasarelas y de los encaminadores, zonas AppleTalk, creación de dominios o grupos de trabajo, relaciones de confianza, etc.
- **Mapa de grupos y usuarios.** Consiste en la descripción de los grupos y usuarios de la red contemplando las posibilidades de acceso a los distintos recursos, así como los derechos de acceso a las aplicaciones, perfiles, privilegios, etc.
- **Mapa de recursos y servicios.** Muestra todos los recursos disponibles identificando sus nombres, el servicio que prestan, el lugar físico o lógico en que residen, los usuarios o grupos a los que se les permite el acceso, el servicio de directorio en el que quedarán publicados, etc.
- **Calendario de averías.** Es el registro de averías del sistema, de modo que permita el análisis de las causas y probabilidad de fallo de los distintos componentes de la red, tanto software como hardware, y su evolución en el tiempo.
- **Informe de costes.** Es el estudio económico tanto del mantenimiento como de las nuevas inversiones del sistema.
- **Plan de contingencias.** Es un documento importantísimo que describe qué hacer y cómo en los casos de situaciones de desastre que se puedan prever. Normalmente este documento se escribe como resultado de la simulación de estas catástrofes y de la experiencia adquirida para la restauración de los servicios. También se suele medir el tiempo de parada en cada una de estas contingencias.

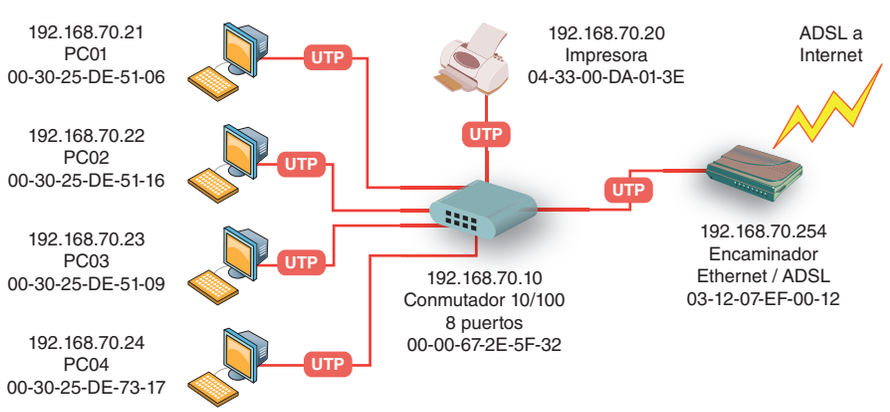


Fig. 8.27. *Diagrama de un mapa físico de red.*

Ampliación

Aplicaciones para la gestión de proyectos

La gestión de un proyecto puede especificarse en un documento electrónico mantenido por una aplicación de gestión de proyectos. En este documento aparecerán las tareas que tienen que realizarse, los plazos que deben respetarse, los recursos humanos o materiales utilizados, el calendario de trabajo, etc.

Se pueden destacar las siguientes dos aplicaciones:

- *Microsoft Project* (software propietario).
- *Planner* (software libre con licencia GPL, **http://live.gnome.org/Planner).**

Ampliación

Aplicaciones para la representación de mapas y gráficos

Los planos y gráficos que representan una red deben registrarse con aplicaciones informáticas apropiadas para ello. Estas aplicaciones se abastecen de gráficos incluidos en librerías gráficas que los mismos fabricantes o desarrolladores ponen a disposición de sus clientes.

Se pueden destacar las dos siguientes aplicaciones:

- *Microsoft Visio* (software propietario, integrado en Microsoft Office).
- *Kivio* (software libre con licencia GPL, **http://www.koffice.org/kivio/**).

Frecuentemente, los mapas de red son documentos muy extensos que, desde luego, no caben en una página de papel impresa.

Esta es la razón por la que estos documentos suelen fraccionarse en múltiples páginas en las que se hacen llamadas de continuidad para saber por dónde sigue cada cable o zona de instalación.

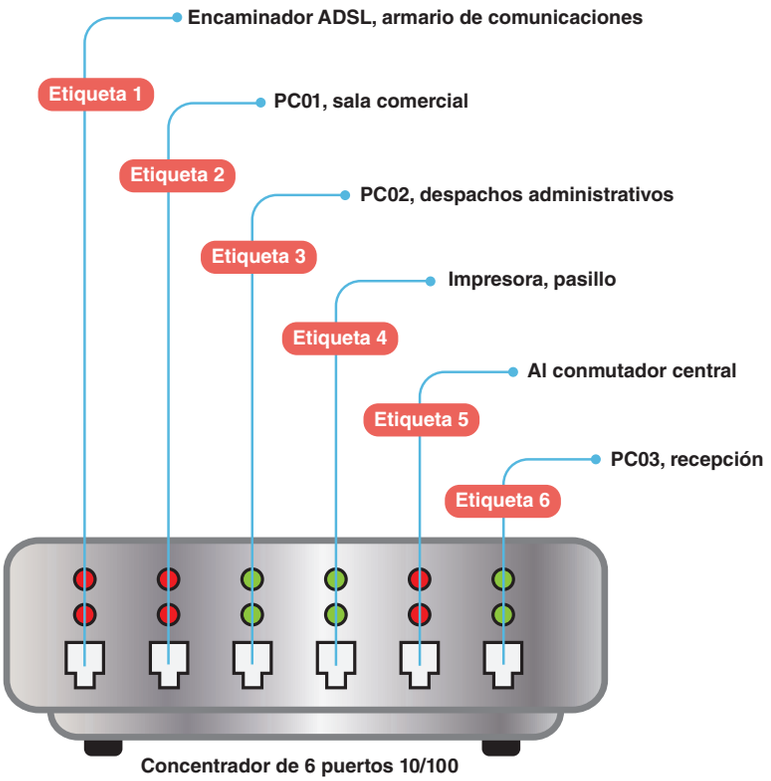


Fig. 8.28. *Mapa lógico de parte de una red.*

Los mapas de red se pueden jerarquizar. En un nivel jerárquico superior, los mapas son gráficos para tener una idea general del aspecto de la red de un simple vistazo.

En los niveles jerárquicos inferiores, en donde se requiere el máximo detalle, los mapas gráficos se pueden sustituir por tablas que organizan la información más estructuralmente.

Actividades

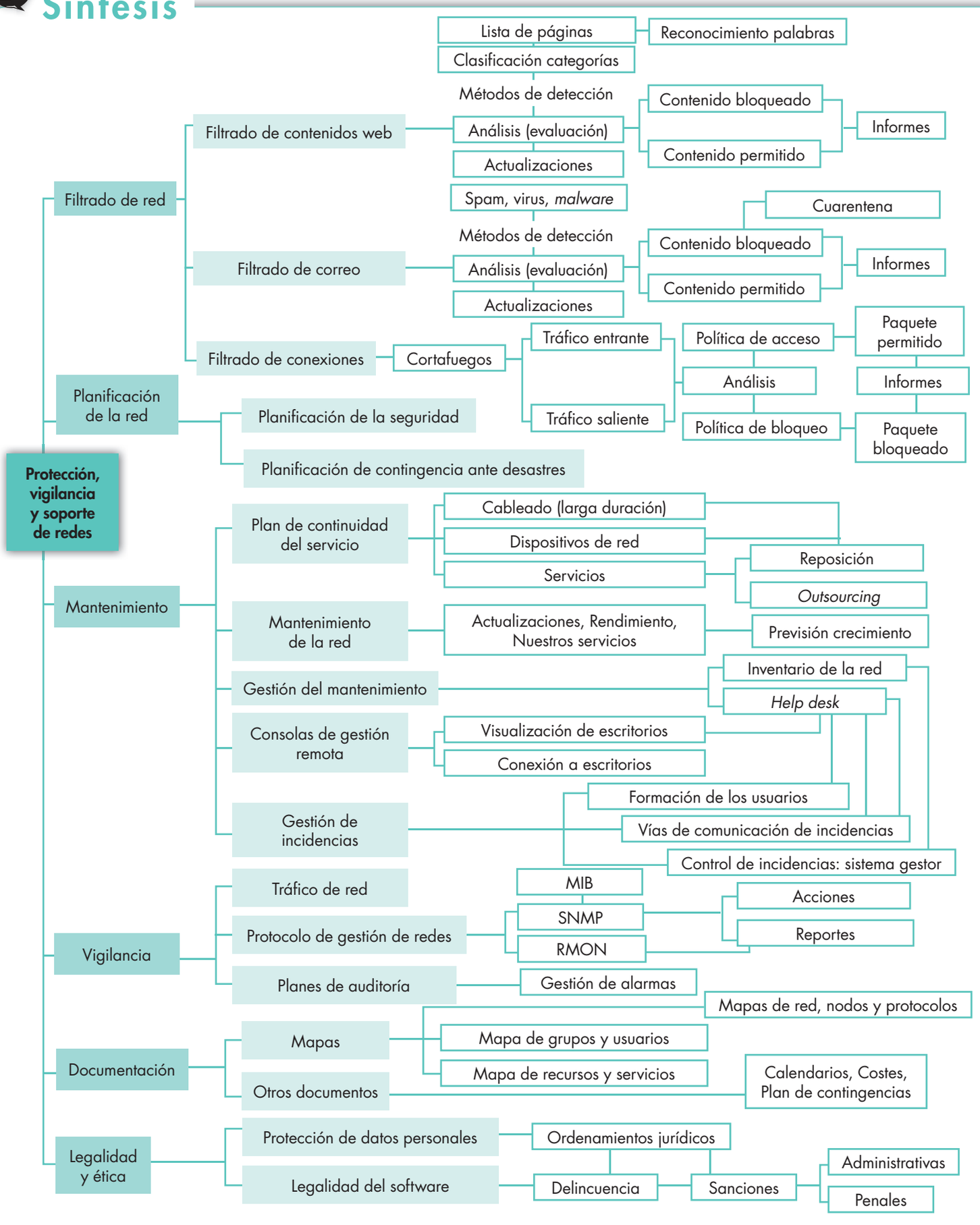
11. Sobre la instalación de red del aula, prepara un calendario anual para la actualización y mejora de los sistemas que componen la red.

12. Conéctate a la web de Ilient, **http://www.ilient.com/,** y descarga la versión gratuita de SysAid, un gestor de ayuda de escritorio *(help desk),* control de inventario *(Asset Management),* monitorización *(monitoring)* y de análisis y reporte, además de un gestor de tareas y proyectos. SysAid gestiona todas estas funcionalidades a través de un portal web. Instala el producto sobre una máquina ayudándote de la documentación que se proporciona en la web. Trata de poner en marcha un sistema de gestión de incidencias.

13. ¿Cuáles son las analogías y diferencias entre los mapas de red y los mapas de nodos?

14. ¿Cuáles pueden ser las razones por las que los documentos que componen una documentación de red tienen que actualizarse frecuentemente?

Síntesis



Test de repaso

1. Relaciona las actividades de la primera columna con el grupo de operación de la segunda.

a) Actualización de sistemas	1) Previsión de futuro
b) Actualización de licencias de software	2) Presupuestos
c) Determinar rendimiento del sistema	3) Calendario de operaciones
d) Fijar fechas límites de ejecución	4) Gestión de proyecto

2. ¿Qué técnica de las que aparecen a continuación no es utilizada por los sistemas de filtrado de contenidos?

a) Comparar las palabras contenidas en las páginas navegadas con un diccionario de palabras prohibidas.

b) Utilizar listados de páginas o sitios prohibidos.

c) Reconocer páginas que están catalogadas para que sean reconocidas como inconvenientes por los navegadores.

d) Filtrar páginas por las direcciones MAC de los servidores que las sirven.

3. ¿Qué técnica de las que aparecen a continuación no es utilizada por los sistemas de detección de virus en correo electrónico?

a) Análisis del cuerpo del mensaje.

b) Análisis de los ficheros adjuntos que lleva incrustados el mensaje de correo.

c) Análisis del servidor de correo desde donde se ha enviado.

d) Impedir que se adjunten ficheros ejecutables.

4. Asocia las características tecnológicas de ambas columnas sobre gestión de consolas remotas y auditorías de la red.

a) RDP	1) Gestión de inventario
b) VNC	2) Gestión de incidencias
c) AIDA64	3) Análisis del sistema
d) OCS ng	4) Conexión de escritorio remoto
e) GLPI	5) Visor de escritorio remoto

5. El documento que especifica qué hacer en caso de sufrir un desastre con los sistemas de información se denomina…

a) Plan de contingencias.

b) Plan de recuperación de licencias.

c) Plan de backups del sistema.

d) Mapa de red.

e) Documento de gestión ética de activos.

6. Un servidor de misión crítica es aquel que…

a) Soporta aplicaciones que cambian constantemente.

b) Ejecuta aplicaciones que no deberían pararse en ningún momento.

c) Gestiona una gran cantidad de trabajo.

d) Ejecuta aplicaciones o servicios con una misión específica.

7. ¿Cuáles de los siguientes protocolos se utilizan para la gestión y monitorización de la red?

a) RMON

b) SMNP

c) SNMP

d) GLPI

8. ¿Cuál de las siguientes funciones es específica del plan de auditoría?

a) Recogida de datos de la red.

b) Confección del mapa de red.

c) Instalación de un software auditor.

d) Gestión contable del consumo eléctrico de los sistemas.

9. ¿Cuál de los siguientes documentos no pertenece específicamente a la documentación de la red?

a) Mapa de red.

b) Mapa de nodos.

c) Mapa de protocolos.

d) Mapa de recursos y servicios.

e) Diagrama de Gantt de la instalación eléctrica.

f) Plan de contingencias de red.

Solución: **1:** a-3, b-2, c-1, d-4; **2:** d; **3:** c; **4:** a-4, b-5, c-3, d-1, e-2; **5:** a; **6:** b; **7:** a y c; **8:** a; **9:** e.

Comprueba tu aprendizaje

I. Entender la necesidad de seguridad en la red proponiendo modos de filtrado que garanticen la legalidad y las actuaciones éticas

1. ¿Qué tipo de filtrado propondrías para limitar las siguientes actuaciones profesionales? Puedes elegir entre filtrado de páginas, de conexiones, de ficheros, de contenidos o de protocolos.
   a) Que no se pueda acceder a la página **www.marca.es**
   b) Qué solo se pueda acceder al servicio web.
   c) Que se pueda utilizar solo correo web.
   d) Que el correo sea solo SMTP/POP.
   e) Que no entre en la red un virus por descarga desde una página web.
   f) Que no se puedan descargar vídeos.
   g) Que no se pueda acceder a ficheros ejecutables.
   h) Que no todas las direcciones IP de la red puedan acceder a un recurso.
2. Naomi es una aplicación de filtrado de contenidos que examina en tiempo real todos los datos que son intercambiados mediante aplicaciones de Internet (navegadores, chats, programas P2P, cliente ftp, etc.). El programa no se limita a una lista negra interna sino que la combina con el análisis heurístico y semántico de las páginas web y enlaces, además reconoce el sistema de etiquetado ICRA. Búscalo en Internet, descárgalo y pruébalo en un equipo de laboratorio.
3. En la página **http://www.archivospc.com/c/904/Filtro+de+contenidos.php** encontrarás una lista de filtros de contenidos. Descarga alguno de ellos y prueba su funcionamiento en laboratorio.
4. Sobre un sistema Linux, instala wireshark y ponlo en ejecución. Ten en cuenta que deberás tener derechos de administración para poder poner la tarjeta en modo monitor y poder escuchar la red. Genera tráfico, por ejemplo navegando por Internet, y comprueba las capturas que wireshark estará haciendo.

   El modo de instalación de wireshark dependerá de la distribución que elijas, pero para Ubuntu o derivados de Debian deberías instalarlo con la orden **sudo apt-get install wireshark.** En los derivados de Red Hat como Fedora la orden es **sudo yum install wireshark.**

II. Identificar las actuaciones de vigilancia y soporte de la red

5. ¿Qué actuaciones profesionales son propias de vigilancia o auditoría y cuáles son de soporte?
   a) Medir el tráfico de red.
   b) Un usuario no puede acceder a su correo electrónico.
   c) Un usuario no puede imprimir por una impresora de red de alto volumen porque ya ha cubierto su cupo mensual de impresión.
   d) El administrador se conecta remotamente a un cliente de la red para examinar la tasa de errores de la interfaz de red.
   e) El administrador se conecta remotamente a un cliente de la red para configurarle el correo electrónico.
6. En la dirección **http://www.lookatlan.com/** tienes una aplicación gratuita *(Look@LAN Network Monitor)* para monitorizar los equipos conectados a una red utilizando varios protocolos de red. Descarga la aplicación e instálala en algún equipo de la red. Sigue su manual online y aprende su funcionamiento.
7. Repite el ejercicio anterior con Host Monitor, una aplicación más profesional. Puedes encontrarla en **http://www.ks-soft.net/hostmon.eng/**

III. Documentar la red

8. Sobre la instalación de red del aula, prepara una documentación completa de los sistemas. Confecciona una carpeta que contenga todos los documentos.
9. Consulta la información de la página **http://www.networkdocumentation.com/** que contiene mucha documentación utilizada por los administradores de red para documentar sus proyectos. Se trata de que te habitúes a leer documentación técnica en lengua inglesa: cuanta más mejor, es el objetivo de este ejercicio.

Unidad 9
Proyecto

En esta unidad aprenderemos a:

- Identificar las fases de un proyecto de instalación de red.
- Advertir la importancia de proveedores, presupuestos y calendarios en cualquier proyecto.
- Diseñar una instalación de red.
- Imaginar posibles mejoras para una instalación de red.

Y estudiaremos:

- Los contenidos de las unidades anteriores en esta obra editorial.
- Algunas utilidades de gestión de proyectos y de confección de croquis.

En esta unidad nos disponemos a integrar todos los conocimientos técnicos adquiridos anteriormente para la consecución de una actuación profesional responsable mediante la formalización de un proyecto.

El contenido de la unidad se divide en tres partes:

- Epígrafe 1. Contiene la exposición del proyecto que resolveremos.
- Prácticas de bloque. Son las actuaciones profesionales concretas sobre el contenido de este módulo que se han ido realizando a lo largo del curso en las prácticas de bloque y que, por tanto, ya se habrán cursado.
- Resto de epígrafes de esta unidad. Contienen las configuraciones finales de la red del proyecto y sus posibles actuaciones de mejora.

1. La necesidad de Torrefría y la respuesta de PHES

Torrefría es una pequeña localidad enclavada en un paso entre montañas que multiplica por cuatro su población en el periodo estival y que tiene una larga historia que se remonta al medievo. Su posición estratégica hizo que desde hace muchos siglos se convirtiera en el centro cultural y comercial de la comarca. Actualmente, la economía de Torrefría se basa en la agricultura y el turismo rural. Además, por lo excepcional de su enclave, no solo tiene mucha historia sino unas buenas comunicaciones con las ciudades cercanas.

Ante las expectativas de crecimiento turístico, el ayuntamiento de Torrefría ha publicado una oferta pública de contratación para la instalación de una biblioteca pública en unos locales anexos al edificio del Ayuntamiento que sirva como sala de lectura y almacenamiento de volúmenes editoriales, punto de conexión a Internet y centro de documentación de historiadores.

La oferta pública especifica lo siguiente:

Excmo. Ayuntamiento de Torrefría

OFERTA PÚBLICA DE CONTRATACIÓN

Proyecto: Tecnificación de la biblioteca del Centro Cívico Torrefría (CCT).

Dotación económica: 30 000 €.

Fecha de adjudicación del concurso: 1 de abril del corriente año.

Fecha límite para la ejecución del proyecto: 3 meses después de la adjudicación.

Presentación de ofertas: Secretaría del Ayuntamiento.

Los proyectos presentados deberán resolver:

1. Diseño e instalación de la red local de la biblioteca del CCT.
2. Instalación de 5 puestos de consulta de fondos y acceso a Internet para la Sala de lectura.
3. Instalación de otros 3 puestos para acceso a los archivos históricos digitalizados y acceso a Internet en la Sala de investigadores.
4. Instalación de 1 puesto para bibliotecario.
5. Infraestructura para acceso a Internet inalámbrico en toda la instalación.
6. Instalación de aire acondicionado.
7. Documento de gestión de seguridad de la instalación de red.
8. Formación y entrenamiento del bibliotecario.

Nota: Los planos de los locales en donde debe hacerse la instalación pueden recogerse en la Secretaría del Ayuntamiento.

PHES, S.L. es una sociedad limitada constituida hace tres años por dos socios, uno de los cuales (el gerente) se ocupa de la labor administrativa, financiera y comercial, mientras que el otro (el técnico) se graduó en los ciclos de Formación Profesional y se ocupa de la parte técnica de los proyectos que los clientes contratan con la empresa.

Además, PHES subcontrata servicios laterales con otras empresas como las de aire acondicionado e instalación eléctrica o con proveedores de materiales y servicios como sistemas de cableado y armarios, canalizaciones o servicios de comunicaciones.

PHES ha recogido de un periódico la oferta del Ayuntamiento de Torrefría. Su gerente, después de una conversación con el técnico de la empresa, ha decidido realizar un proyecto que presentará a concurso.

Si ganan el concurso, PHES se encargará del diseño e instalación de la red y subcontratará aquellos elementos de la instalación que no son específicos de su actividad directa, por ejemplo, la instalación eléctrica o el aire acondicionado.

El gerente de PHES ha recogido en el Ayuntamiento los planos de la localización de la instalación. Se trata de un edificio con una planta baja de 8×10 metros cuadrados y una media planta alta de 3×10 metros cuadrados. Las dos plantas se comunican por una escalera de caracol. La planta baja deja acceso en su entrada a unos cuartos de baño y a la Sala de fondos en donde se ubican las estanterías con los volúmenes de la biblioteca, pero que no tienen relevancia en el proyecto, puesto que aquí se trata solo de informatizar la Sala de lectura (planta baja) y la Sala de investigadores (planta alta). La planta alta tiene un balconcillo asegurado con una barandilla con visión directa de la planta baja.

La entrada de servicios (telefonía, corriente eléctrica) de la edificación tiene una entrada por uno de los ángulos del edificio.

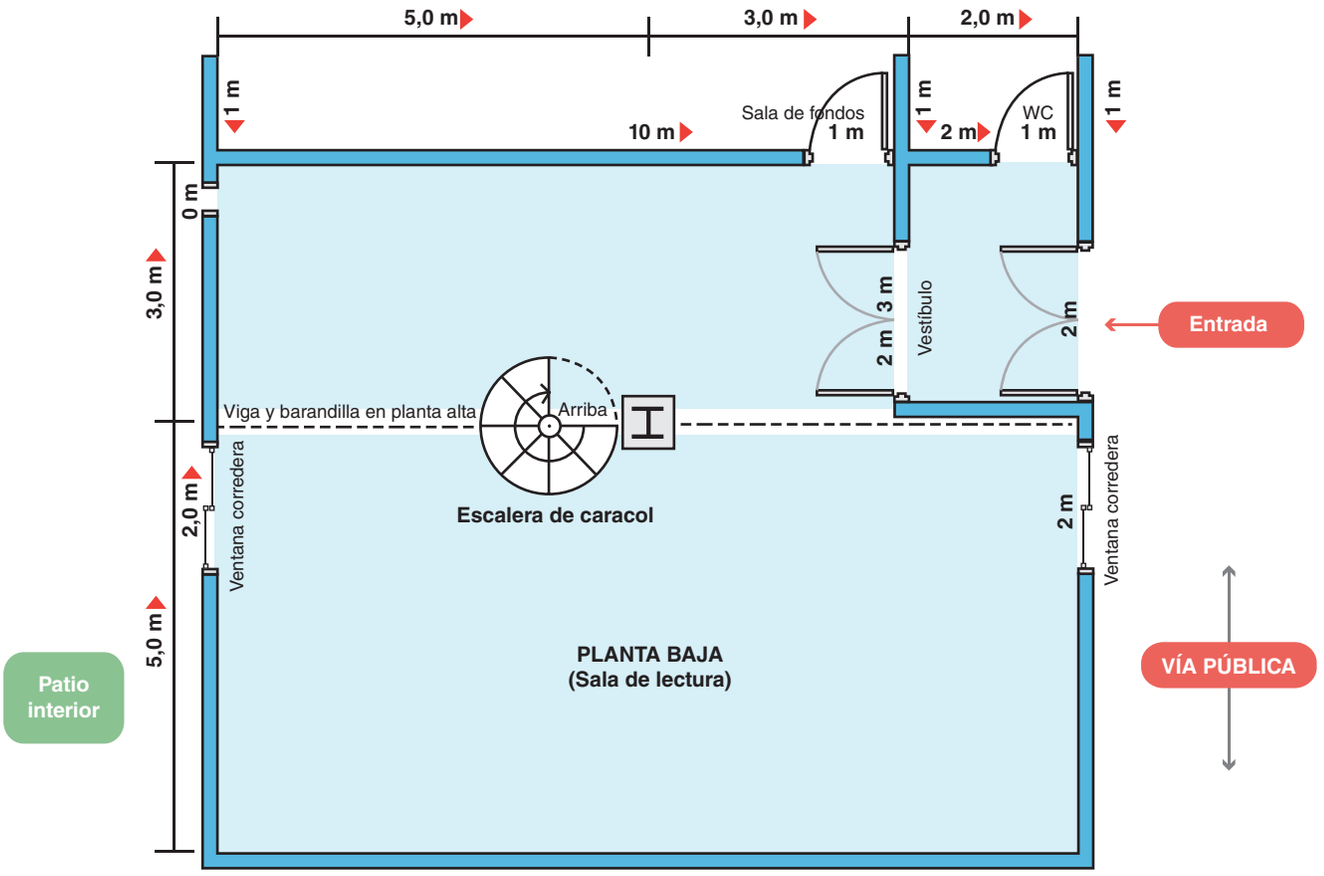


Fig. 9.1. *Planos de la localización de la biblioteca del CCT: planta baja.*

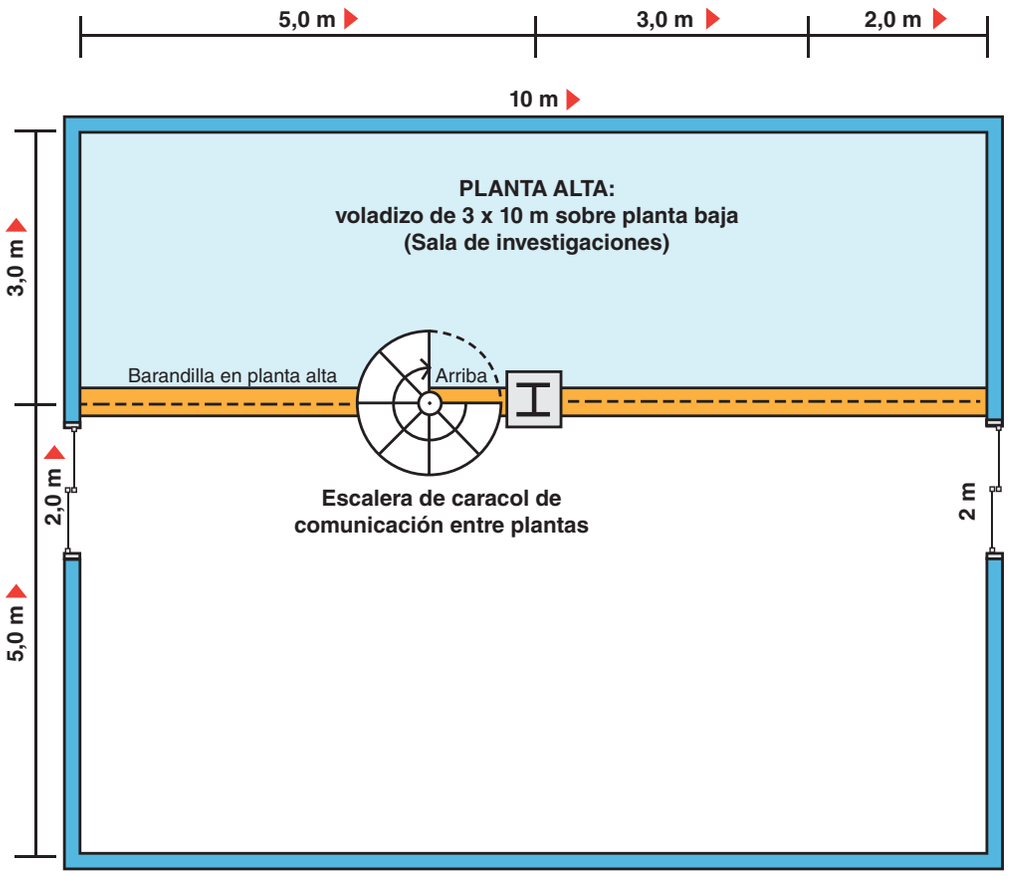


Fig. 9.2. *Planos de la localización de la biblioteca del CCT: planta alta.*

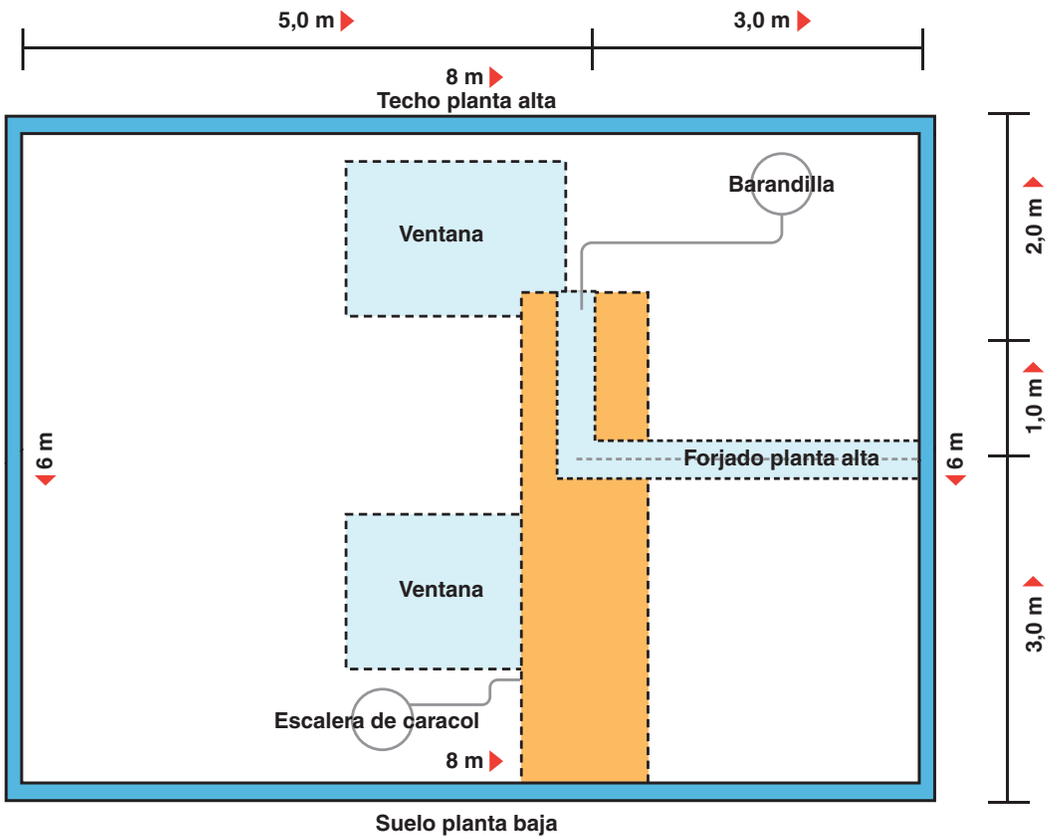


Fig. 9.3. *Planos de la localización de la biblioteca del CCT: alzado visto desde el muro de entrada.*

1.1. Fases del proyecto

PHES se ha planteado dos fases para el proyecto: en primer lugar la elaboración del proyecto de concurso y en segundo lugar, si lo gana, la ejecución del proyecto de instalación.

A. Elaboración del proyecto de concurso

En esta fase se realizarán los pasos A1-A8 que se especifican en la Tabla 9.1.

B. Ejecución del proyecto

Si gana el concurso, PHES firmará el contrato con el Ayuntamiento de Torrefría y se dispondrá a su ejecución en los términos establecidos por la oferta pública de contratación. En esta fase se dispondrán los pasos B1-B9 enumerados en la Tabla 9.1.

A1. Recogida de documentación y búsqueda de proveedores y profesionales.	B1. Establecimiento de la fecha inicial del proyecto.
A2. Presentación de una propuesta técnica.	B2. Realización de pedidos a proveedores.
A3. Análisis de fortalezas y debilidades.	B3. Entrada de profesionales subcontratados: aire acondicionado, canalizaciones e instalación eléctrica.
A4. Ajuste de la propuesta.	B4. Instalación del cableado de red.
A5. Mapa de profesionales.	B5. Instalación de los equipos informáticos: servidores.
A6. Elaboración de un presupuesto.	B6. Instalación de las comunicaciones externas.
A7. Elaboración de un calendario.	B7. Instalación de clientes y de otros dispositivos de la red.
A8. Confección del proyecto y presentación a concurso.	B8. Elaboración de la documentación.
	B9. Formación y entrenamiento.

Tabla 9.1. *Detalle de las fases del proyecto.*

Las etapas de la primera fase (A1 a A8) hay que hacerlas secuencialmente, salvo la búsqueda de proveedores y profesionales que se puede distanciar más en el tiempo, pero siempre antes de la etapa de presupuesto.

En la segunda fase (B1 a B9), una propuesta de ejecución podría ser la siguiente:

- Lo primero es B1. En función de esa fecha se tiene que hacer B2 para que los proveedores suministren el material necesario con la suficiente antelación. Seguidamente se procede a la etapa B3.
- Mientras B3 no se finalice no se pueden iniciar las etapas siguientes, salvo B5 y B7 cuya configuración de equipos puede realizarse en las instalaciones de PHES y llevar los equipos ya configurados a la instalación final para su prueba.
- B6 se puede realizar en cualquier momento después de B3, pero hay que tener en cuenta los tiempos de espera hasta que los proveedores de comunicaciones nos sirvan los servicios que contratemos.
- B8 debe hacerse a lo largo de todo el proyecto, aunque solo al final de este se plasmarán en documentos listos para imprimir.
- B9 es la etapa final.

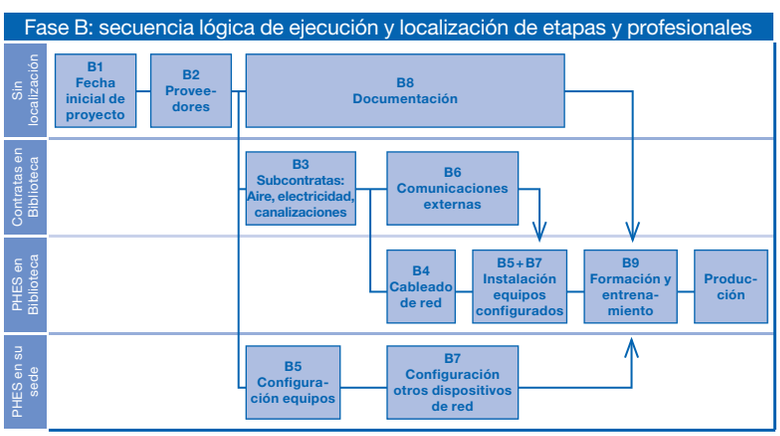


Fig. 9.4. *Secuencia lógica de las etapas de la fase B.*

1.2. Localización en este libro de texto de la resolución de cada tarea

Las tareas para la presentación y ejecución del proyecto se irán resolviendo con cierto detalle en las prácticas de final de bloque a lo largo del libro. En el texto iremos reproduciendo las tareas de los dos socios de PHES en la ejecución de su trabajo ordinario. Cada tarea se localizará en este libro de texto como se indica en la Tabla 9.2.

Fases/Etapas de proyecto	Bloque en el libro	Observaciones
A1 - A8	1	Elaboración del proyecto de concurso.
B1 - B4	1	Aprobación del proyecto y comienzo de ejecución. Canalizaciones y cableado.
B5	2	Configuración de red en equipos. Servicios básicos de red.
B7 (1.ª parte)	2	Configuración de impresoras de red.
B7 (2.ª parte)	3	Configuración de los conmutadores. Configuración de la videocámara. Configuración del punto de acceso inalámbrico.
B7 (3.ª parte)	Unidad final	Configuración de las estaciones cliente.
B6	Unidad final	Configuración del encaminador ADSL. Configuración del proxy/cortafuegos.
B8 - B9	Unidad final	Documentación, formación y entrenamiento. Propuestas de mejoras de la instalación.

Tabla 9.2. *Localización en este libro de las tareas en las dos fases del proyecto.*

MUY IMPORTANTE, ANTES DE SEGUIR:

La secuencia lógica para seguir ordenadamente el desarrollo de esta práctica implica haber comprendido la realización en laboratorio de las tareas ejecutadas en las prácticas de final de bloque anteriores.

Solo después, la continuación de la lectura en esta unidad puede resultar provechosa.

2. Configuración de los equipos cliente

Puesto que ya tenemos los servicios de infraestructura (DHCP y DNS) y de usuarios (impresoras y carpetas de red) funcionando, podemos configurar la red en las estaciones cliente.

Los datos relevantes para esta configuración son los que se especifican en la Tabla 9.3.

CLIENTES	FIJOS o de sobremesa	MÓVILES o inalámbricos
WINDOWS O LINUX	IP estática Máscara: 255.255.255.0 DNS: 182.168.1.10 Puerta defecto: 192.168.1.100 Proxy: no necesita.	IP dinámica (por DHCP) Máscara: 255.255.255.0 DNS: 182.168.1.10 Puerta defecto: No se asignará. Proxy: 192.168.1.100, puerto 8080.

Tabla 9.3. *Parametrización de red para los equipos cliente.*

Tenemos que hacer dos observaciones interesantes:

1. A los clientes móviles no les hemos asignado la puerta por defecto. Es una medida de seguridad. Si quieren navegar pueden hacerlo configurando su proxy a la dirección y puerto de escucha del proxy que instalaremos (IPCOP), pero como este será un proxy web, solo permitirá el acceso a Internet mediante los protocolos de navegación habituales. Si un cliente móvil está infectado por un virus, este lo tendrá más difícil para salir a Internet puesto que no sabe dónde está Internet (esto es lo que le indicaría la puerta por defecto). Esta es la configuración que asignará al portátil el servidor DHCP instalado en la práctica de bloque 2.
2. Los clientes fijos sí tienen puerta por defecto porque son los equipos de nuestra instalación que llevarán antivirus. Para ellos no será necesario configurar el proxy en su navegador con tal de que el servidor proxy que instalemos tenga también la funcionalidad de proxy transparente, que es el caso de IPCOP. El acceso a Internet desde estos equipos podrá, por tanto, ser más completo. Las configuraciones de los equipos fijos se harán todas manualmente.

2.1. Clientes móviles inalámbricos

Como los clientes inalámbricos no tendrán que configurar la red, bastará con que se conecten a ella a través del punto de acceso inalámbrico. Para ello, es suficiente con que exploren las redes inalámbricas y se conecten a la Wi-Fi de la biblioteca asignando la clave WEP que les proporcionará el bibliotecario. Sus parámetros de red serán asignados automáticamente mediante DHCP, por tanto, la red deberá ser configurada siguiendo la secuencia de la Fig. 9.5.

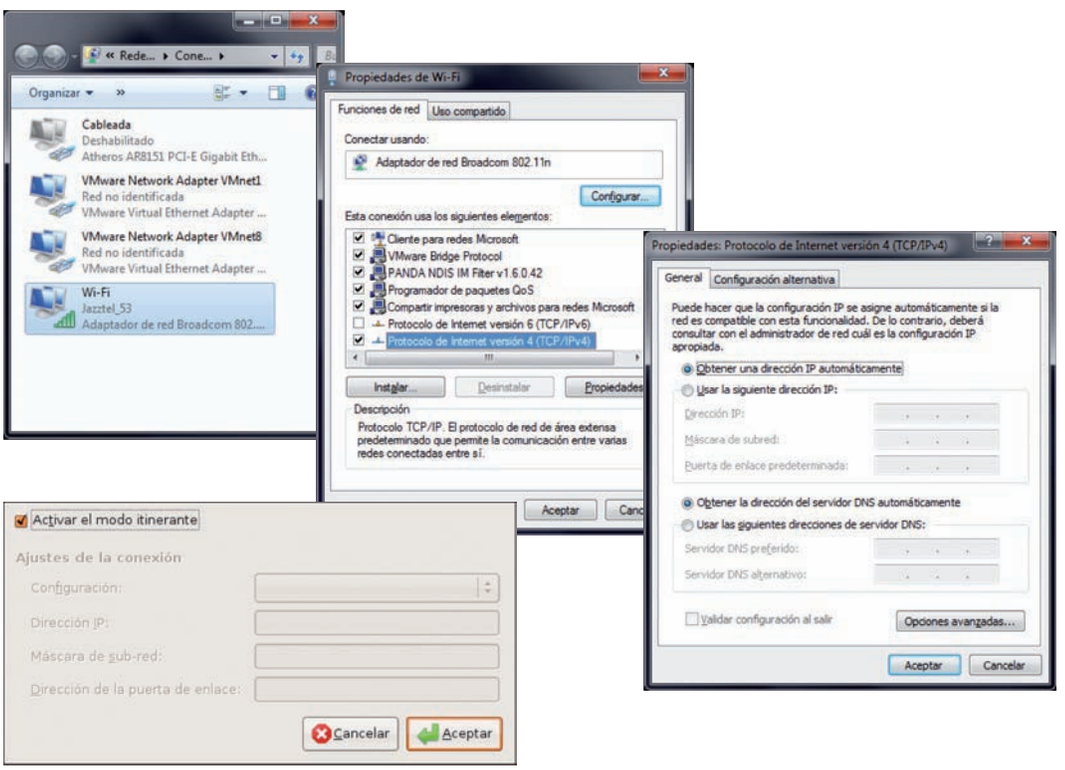


Fig. 9.5. *Arriba, secuencia de asignación por DHCP en una interfaz Windows inalámbrica. Abajo, la ficha equivalente en Ubuntu (modo itinerante).*

Por otra parte, para poder navegar bastará con que configuren su explorador de Internet para que apunte al servidor proxy con dirección 192.168.1.100 y puerto 8080 (Fig. 9.6).

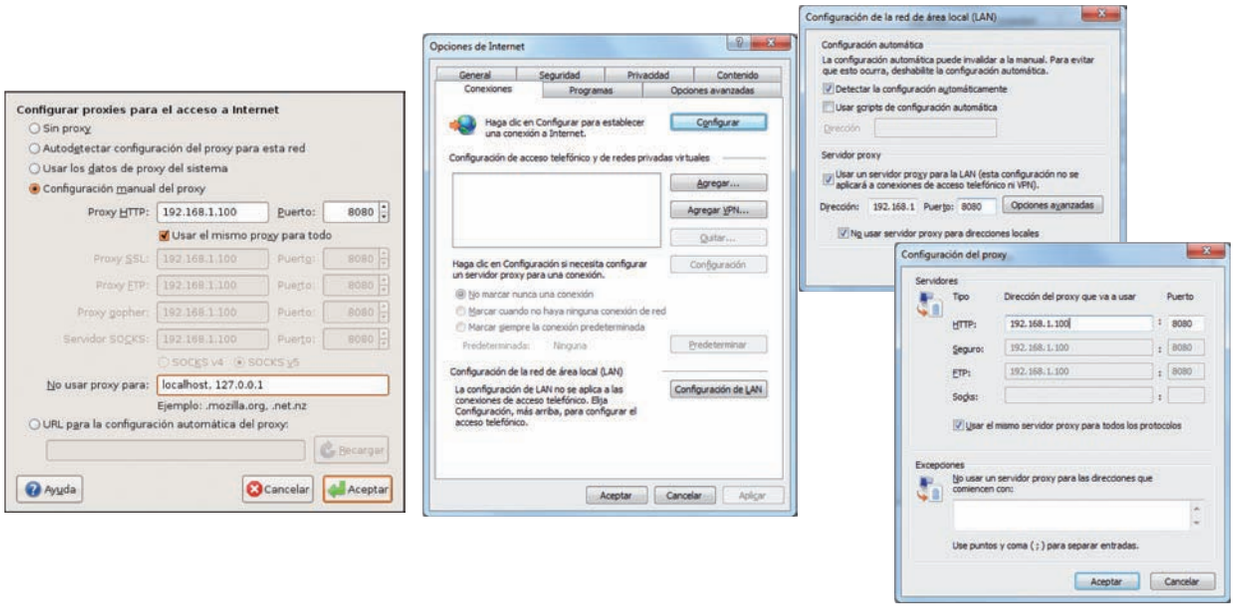


Fig. 9.6. *A la izquierda, configuración sobre Firefox de un cliente móvil inalámbrico sobre Linux. A la derecha, su equivalente sobre Internet Explorer.*

2.2. Clientes fijos

Como los clientes fijos se configurarán manualmente, bastará con abrir las fichas de red de cada uno de los equipos y configurar en cada uno su dirección IP, máscara, puerta por defecto y DNS según la documentación del proyecto que ya concretamos en la práctica de bloque 2.

En un cliente Linux la secuencia de configuración es la que se puede ver en la Fig. 9.7, en donde se ha configurado la estación PCB2.

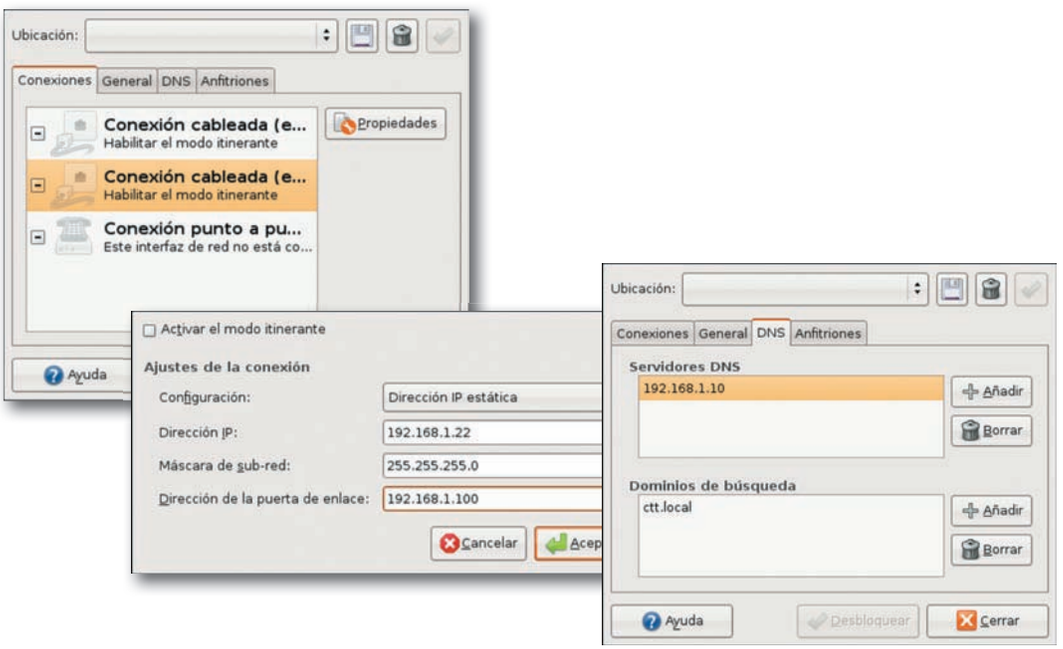


Fig. 9.7. *Configuración de la red en un cliente Linux fijo.*

En un cliente Windows la configuración de red ya es conocida. Por ejemplo, para configurar PCA1, que tiene por dirección 192.168.1.31, tendremos que seguir la secuencia de la Fig. 9.8.

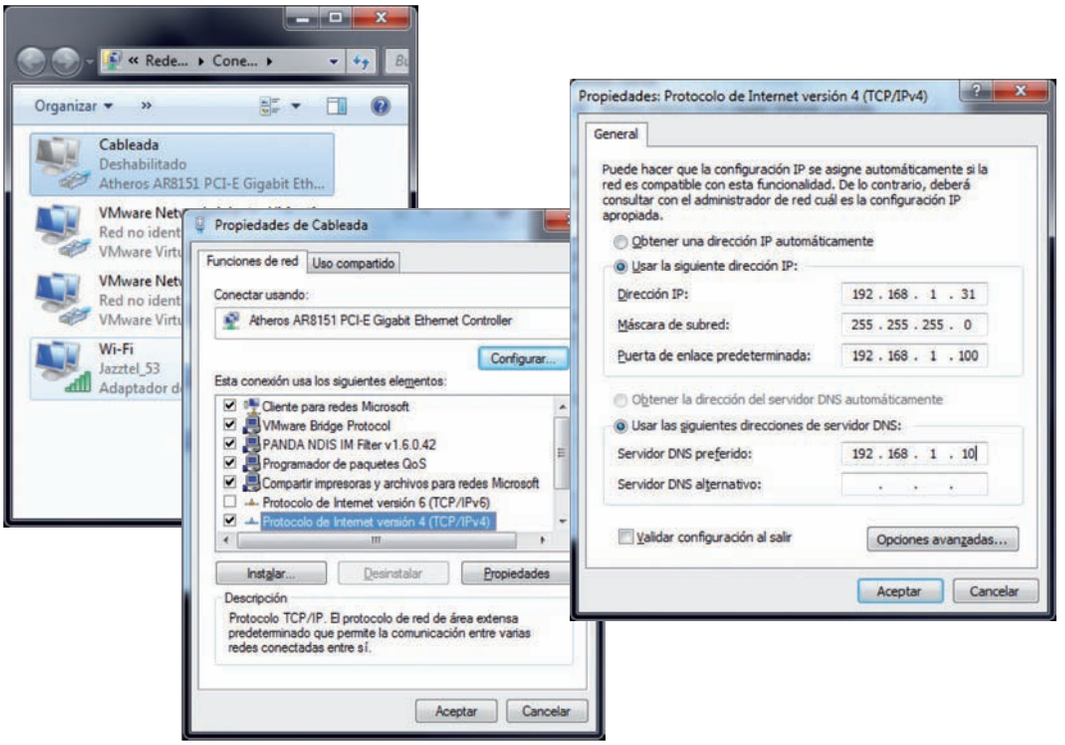


Fig. 9.8. *Configuración de la red en un cliente Windows fijo.*

Con la configuración de clientes realizada hasta ahora, todas las estaciones de la red podrán acceder a los recursos locales para los que tienen derechos de acceso. Sin embargo, para navegar, los clientes móviles tendrán que configurar su navegador para que apunte al servidor proxy de la red, mientras que los clientes fijos no tendrán que hacer ninguna configuración adicional puesto que utilizarán un proxy transparente (Fig. 9.9).

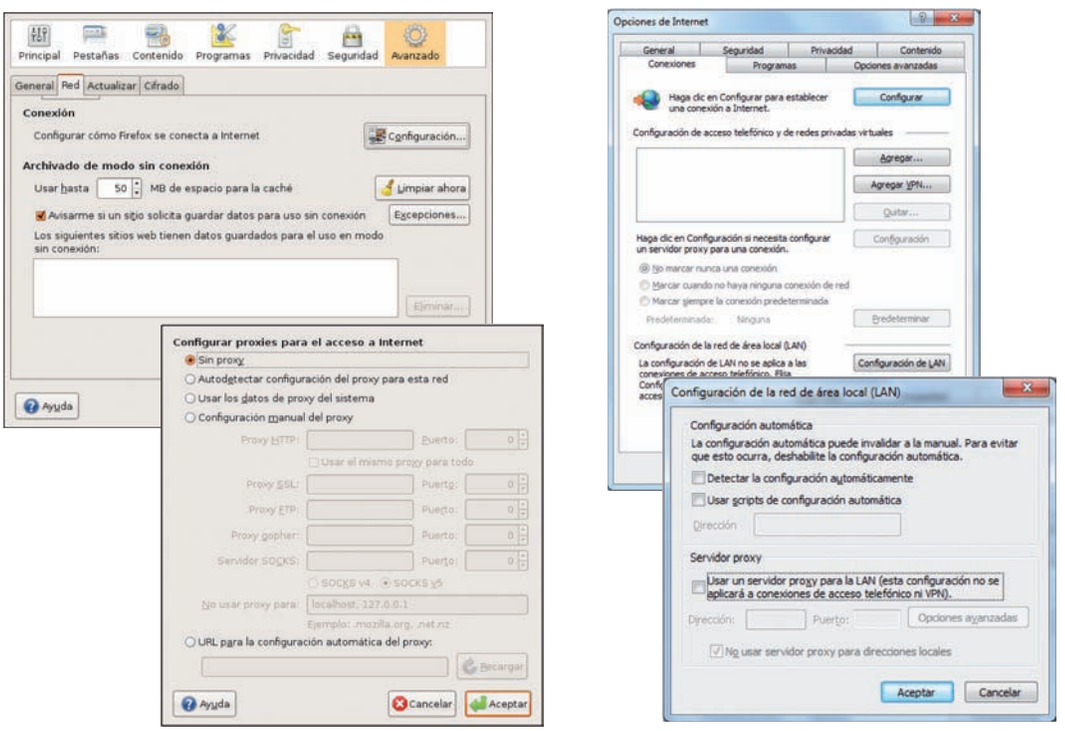


Fig. 9.9. *A la izquierda, configuración sobre Firefox de un cliente fijo. A la derecha, su equivalente sobre Internet Explorer.*

Truco

El fabricante del router habrá configurado una dirección IP de fábrica, que vendrá especificada en el manual del encaminador, así como un nombre de usuario administrador y contraseña inicial. Conectaremos el router directamente a la interfaz de red de un PC, pondremos en esta interfaz una dirección compatible con la que trae el router de fábrica y nos conectaremos a él a través de su dirección mediante el navegador web. Sobre esta página, estableceremos la dirección IP final del router y a partir de ese momento ya podremos conectar el router a nuestra LAN y terminar de gestionarlo a través de su dirección definitiva.

3. Configuración del encaminador ADSL

En el encaminador ADSL, el procedimiento consistirá en conectarse al servidor web que incorpora para establecer en él unas direcciones que estén de acuerdo con la especificación de nuestro proyecto.

El proveedor de Internet nos tiene que especificar la parametrización de la red WAN del router: protocolos, direcciones IP, máscaras, puerta por defecto, etc.

Tenemos que observar (Fig. 9.10) cómo hemos rellenado los parámetros de la WAN con los valores proporcionados por el fabricante. Por ejemplo, los servidores DNS son los valores que establecimos como reenviadores en nuestro servidor DNS. El *gateway* (213.97.119.130) es el enrutador del proveedor que nos conecta a Internet.

En la configuración de la LAN, estableceremos que la dirección IP local del router es 10.1.1.1, lo que habíamos previsto en la definición del proyecto.

Hay muchos otros parámetros que se pueden configurar, pero lo que hemos visto hasta aquí es lo específico de la función de enrutamiento. Otros valores pueden indicarle al router que ponga en marcha un sencillo cortafuegos, que admita conexiones VPN, etc.

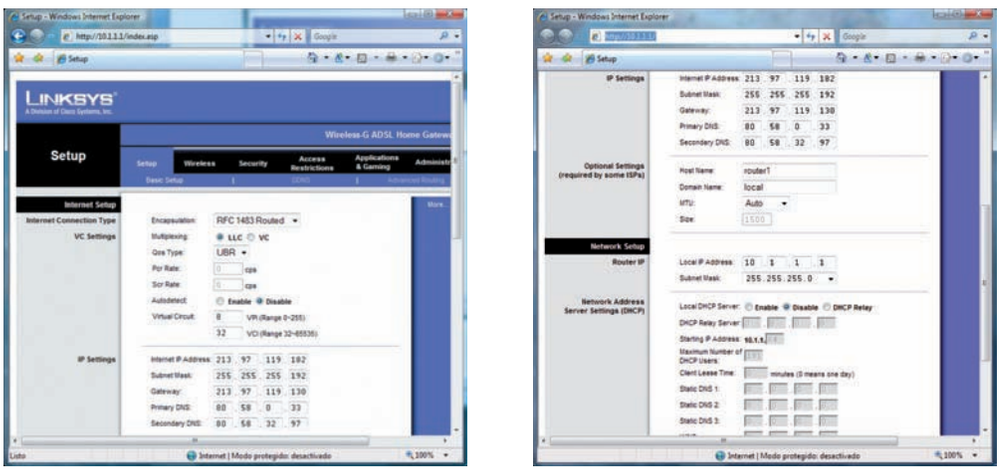


Fig. 9.10. *Ventanas de configuración de los parámetros de red de las dos interfaces de un encaminador ADSL: WAN a la izquierda y LAN a la derecha.*

Claves y consejos

También se podría utilizar IPFire, un producto semejante que se puede descargar de **http://www.ipfire.org/**

4. Configuración del servidor proxy web

IPCOP es una distribución de Linux específica para la construcción de cortafuegos que incorpora un servidor web para que las opciones del cortafuegos se puedan configurar mediante una página web. Realmente, IPCOP es un gestor web de iptables sobre Linux. IPCOP incluye un servidor proxy web que puede funcionar también en modo transparente.

IPCOP se puede descargar de **http://www.ipcop.org/,** en donde también se puede encontrar mucha información sobre cómo instalarlo y configurarlo.

El procedimiento de instalación que hemos elegido está soportado sobre un PC (que puede ser muy básico), con dos interfaces de red: LAN y WAN. Cuando arrancamos del CD que contiene la distribución IPCOP, el sistema nos preguntará qué tipo de IPCOP queremos y los parámetros de red de las redes. Nosotros elegiremos un IPCOP de dos redes (*green* y *red*, que es como IPCOP identifica a la LAN y WAN respectivamente). Estableceremos en estas dos redes los parámetros de la Tabla 9.4.

Nombre equipo	IP	Máscara	Ruta por defecto	Observaciones
IPCOP	Interna o *green* (verde): 192.168.1.100 Externa o *red* (roja): 10.1.1.100	Interna: 255.255.255.0 Externa: 255.255.255.0	10.1.1.1 (al encaminador ADSL)	Puerta por defecto de IPCOP dirigido al encaminador ADSL.

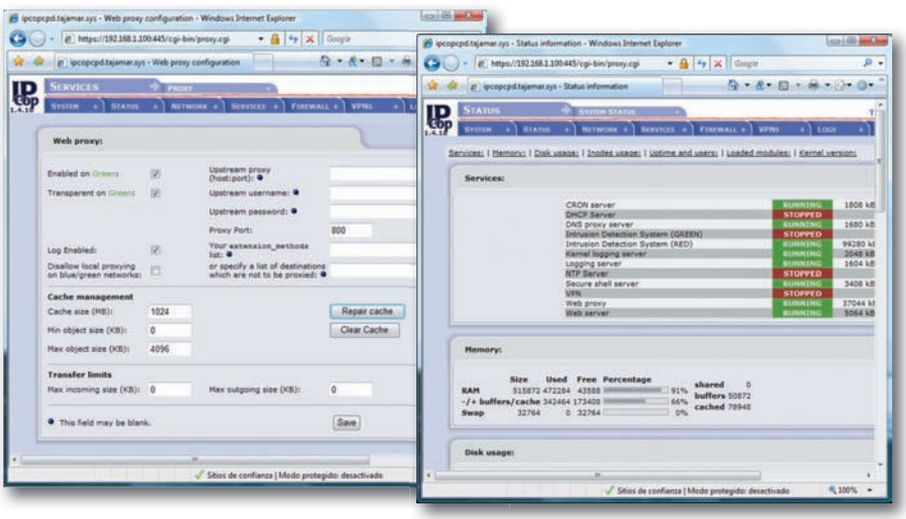
Tabla 9.4. *Parámetros de red de las dos interfaces del cortafuegos IPCOP.*

Después de la instalación de IPCOP con estos parámetros ya nos podremos conectar a él por la dirección 192.168.1.100 o por su equivalente nombre *dns*: *ipcop.ctt.local* mediante el navegador web utilizando https por el puerto 445, por tanto, el URL de conexión será **https://ipcop.ctt.local:445/** o **https://192.168.1.100:445/**

Una vez que obtengamos la página de administración de IPCOP ya podremos hacer desde ella el ajuste fino del equipo.

Para nuestro propósito, solo tendremos que configurar el servidor proxy para que admita las conexiones de nuestros clientes por la red LAN *(green network)* y las pase hacia el encaminador ADSL *(red network)*. La página de configuración del servidor proxy está accesible desde el menú web de la página de administración de IPCOP.

Obsérvese cómo se han habilitado los dos proxys (el transparente y el no transparente). El transparente recibirá cualquier petición web por su interfaz LAN (*green*) y el cliente solo tendrá que tener habilitada su puerta por defecto apuntando a esta interfaz LAN (192.168.1.100), justo como nosotros hemos configurado la red para los clientes fijos.



En el caso del proxy no transparente, las peticiones se recogerán también en la LAN, pero solo por el puerto que se especifica (el 800 en la figura). Como la especificación de nuestra red es que los clientes móviles puedan utilizar este proxy no transparente por el puerto 8080, tendremos que sustituir el valor 800 por 8080, guardaremos los cambios y ya tendremos configurado el proxy en nuestra red. A partir de este momento, todos los clientes de nuestra red LAN podrán navegar.

Fig. 9.11. *Configuración del servidor proxy de IPCOP (izquierda). Vista de los servicios que proporciona IPCOP y su estado (derecha).*

5. Documentación, entrenamiento y formación

Toda la documentación de la red se ha ido escribiendo conforme hemos ido realizando el proyecto, precisamente porque lo hemos hecho de un modo ordenado. De hecho, hemos creado la documentación en primer lugar y luego hemos ido ejecutando cada tarea de acuerdo con lo que la documentación especificaba que teníamos que hacer.

Una recopilación de las tablas y las figuras de configuración de esta unidad y las prácticas de final de bloque son la base de una buena documentación de la red, puesto que todo lo que se ha realizado está documentado y organizado por tareas específicas: planos, medidas de cables, cómputo de rosetas, equipos y configuraciones.

El plan de formación tiene como objetivo que los usuarios sepan utilizar la red y lo hagan eficientemente. Se pueden definir dos perfiles de formación: los usuarios del servicio de biblioteca (lectores o investigadores) y el bibliotecario. Sin embargo, en cuanto al entrenamiento se refiere, solo se puede disponer de unas horas de formación para el bibliotecario. Los usuarios futuros de la biblioteca no estarán disponibles para su formación en el momento en que esta se debe impartir. La formación de estos usuarios descansará también en la figura laboral del bibliotecario.

El plan de entrenamiento de los usuarios de la biblioteca se reducirá a que el bibliotecario, una vez que haya recibido su propia formación, elabore unos documentos muy sencillos, asequibles al perfil de los usuarios de la biblioteca, que expliquen el modo de utilización de los servicios:

1. Cómo hacer las conexiones inalámbricas.
2. Cómo abrir unidades compartidas en la red.
3. Cómo imprimir a través de las impresoras compartidas.
4. Cuál es la cuenta de usuario que pueden utilizar para acceder a los servicios del servidor.
5. Cómo deben configurar el proxy de su navegador para que puedan acceder a Internet.
6. Cómo deben configurar los parámetros de red.
7. Advertencia sobre el código ético que debe seguirse en la utilización de las instalaciones y en el acceso a Internet.

El plan de entrenamiento del bibliotecario es un poco más extenso porque debe conocer no solo lo que se ha expuesto anteriormente para el resto de usuarios, sino además:

8. Los servicios que provee la red (carpetas e impresoras).
9. Encender y apagar los servidores y el resto de los equipos.
10. Examinar la videocámara.
11. El sistema de gestión de cuentas: usuarios, contraseñas, etc.
12. ¿Qué hacer en caso de avería de algún equipo? (lo habitual sería que PHES ofreciera al Ayuntamiento de Torrefría un contrato de mantenimiento).
13. ¿A quién acudir frente a una interrupción del servicio de Internet?

6. Propuesta de posibles mejoras

El proyecto ha sido finalizado, pero siempre conviene reflexionar, una vez concluido, para evaluar posibles mejoras para la instalación o simplemente modos en que el proyecto podría mejorarse en el futuro.

Algunas de las propuestas de mejora y ampliación podrían ser las siguientes:

- Puesto que SRV tiene dos interfaces de red (una la teníamos desactivada porque no la utilizaríamos), podríamos ensayar una solución de virtualización para IPCOP (que necesita dos interfaces de red) de modo que IPCOP y SRV compartan el mismo hardware. De este modo nos ahorraríamos el coste del hardware de IPCOP. La propuesta de virtualización se puede hacer sobre Microsoft Hyper-V, sobre VMWare o incluso sobre VirtualBox (todas estas aplicaciones de virtualización son gratuitas, aunque no con una licencia libre). También hay otras posibilidades que se desarrollan sobre software libre.
- De acuerdo con esto, también podríamos eliminar el conmutador de la planta alta puesto que nos sobran puertos de comunicaciones en el de la planta baja. Los cables de red de la planta alta ahora tendrían que prolongarse verticalmente hasta el conmutador de la planta baja por el segmento de canaleta por el que se comunicaban ambos conmutadores. Esto incrementa algo el coste en cable de red, pero salimos beneficiados porque ya no nos haría falta ni el *switch* de planta alta ni tampoco el armario de comunicaciones.
- Si eliminamos el armario superior, la red que llega a la videocámara y al punto de acceso ahora se podría distribuir desde la planta baja con un ramal vertical de canaleta por el ángulo de la estancia justo debajo de estos dos dispositivos.

Con lo que nos ahorraríamos con estas mejoras, podríamos adquirir un SAI para el conjunto virtualizado SRV+IPCOP y, aun así, nos sobrarían más de 1 000 €, que sobre los 30 000 € de dotación supondrían unos beneficios del 3,3 % superior al inicial, añadiendo la mejora del SAI y sin disminuir los servicios prestados.

El siguiente paso en la mejora del sistema consistiría en abrir la red al exterior mediante conexiones VPN o la publicación de los fondos a través de un servidor web instalado en SRV hacia la web. Estas dos mejoras serían gratuitas puesto que SRV tiene IIS (servidor web de Microsoft) e IPCOP puede hacer la publicación de este servidor y gestionar las VPN, pero estas mejoras deben ser objeto de un curso más avanzado.

7. Casos de estudio

En los casos de estudio que se proponen a continuación se hacen dos propuestas de software libre para poder ser utilizadas a bajo coste en instalaciones de pymes.

La propuesta es el estudio de las características y modo de instalación de las dos distribuciones Linux de valor añadido que se proponen (Untangle y Zentyal) y que se asimilarán en los dos casos de estudio siguientes, para ensayar despliegues concretos de una de estas distribuciones o ambas a la vez con el objetivo de dar solución a los problemas reales de una pyme.

Como ejercicio, se propone tener una entrevista con algunas pymes, hacer un análisis de sus características, problemas y necesidades e intentar ensayar con Untangle y Zentyal (u otras distribuciones conocidas anteriormente a lo largo del texto del libro) una solución a la problemática que presente la pyme que se considere más adecuada.

CEO

SMR_RL_AAbad_09_Instalacion Untangle.pptx

Documento que contiene información sobre las características e instalación de Untangle (89 diapositivas autocomentadas en las páginas de notas de la presentación).

Caso de estudio 1: Untangle

Untangle es una solución open source para la instalación de un *gateway* en una caja *(box)* para realizar las siguientes funciones:

- Filtrado de contenidos, correo spam.
- Control de red y gestión del ancho de banda.
- Gestión de usuarios.
- Otros servicios de red como DNS, DHCP, QoS, NAT, etc.
- Permite muchos módulos de software añadidos bajo pago en las versiones *Standard* y *Premium*.
- La versión Lite es totalmente gratuita.

Untangle se puede descargar desde **http://www.untangle.com/Download-Untangle**

Se propone la instalación y el estudio de Untangle siguiendo las indicaciones que se ofrecen en el documento PowerPoint que se cita en el CEO situado al margen.

Fig. 9.12. *Vista de la consola de administración de Untangle.*

Caso de estudio 2: Zentyal

Zentyal es una distribución *open source* basada en Ubuntu Server que proporciona soluciones para pymes en los siguientes escenarios:

- *Gateway* de acceso.
- Servidor de seguridad (UTM).
- Servidor departamental de oficina.
- Servidor de infraestructura de red.
- Servidor de comunicaciones.

Zentyal se puede descargar desde **http://www.zentyal.org/downloads**

Se propone la instalación y el estudio de Zentyal siguiendo las indicaciones que se ofrecen en el siguiente documento:

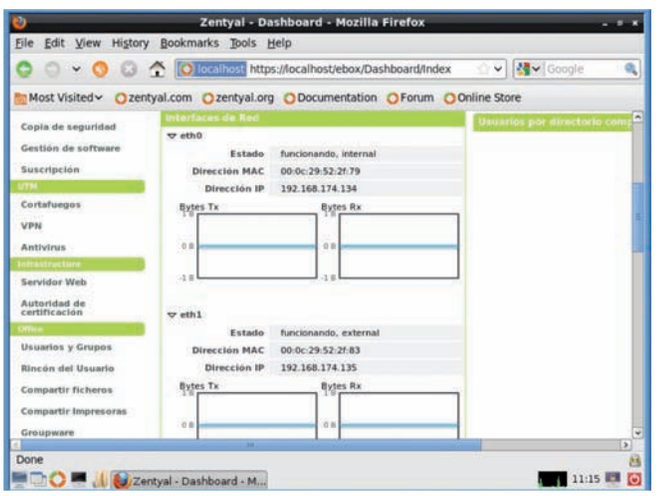


Fig. 9.13. *Vista de la consola web de administración de Zentyal.*

CEO

SMR_RL_AAbad_09_InstalacionZentyal.pptx

Documento que contiene información sobre las características e instalación de Zentyal (60 diapositivas autocomentadas en las páginas de notas de la presentación).

Glosario

A

Arquitectura de una red. Conjunto organizado de capas y protocolos que la red utiliza para producir sus comunicaciones entre nodos.

Auditoría del sistema. Es la configuración de registros y alarmas que nos advierten del estado del sistema en todo momento. De este modo, el sistema irá dejando registro de cuantos errores o acontecimientos ocurran en él.

Aplicaciones de misión crítica. Son aquellas que no pueden dejar de funcionar sin un gran impacto sobre la producción global de la empresa. Una aplicación de misión crítica no puede pararse.

Analizador de red o *sniffer*. Escuchador de la red que espía todo el tráfico que pasa por el segmento de red en que se instala con objeto de analizar lo que circula por la red.

B

***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 conmutadores 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.

***Blacklist* o lista negra.** 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.

Bloque de datos. Conjunto de datos que posee una estructura interna perfectamente definida.

C

Cableado estructurado. Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. La instalación de estos elementos debe respetar los estándares previstos para que un despliegue de cableado se pueda calificar como de cableado estructurado.

Cable apantallado. Aquel que está protegido de las interferencias eléctricas externas por acción de un conductor eléctrico externo al cable, por ejemplo, una malla metálica. Esta malla también impide que el cable produzca interferencias en su entorno.

Capa o nivel. Cada una de las subdivisiones funcionales de una arquitectura de red.

Conector. También llamado interfaz físico, es un dispositivo que sirve para unir circuitos eléctricos.

Colisión de red. Es el fenómeno de interacción de dos señales que se produce cuando las tramas procedentes de dos equipos se vuelcan simultáneamente sobre el mismo canal en la misma banda de frecuencia.

Colisión, dominio de. Es la porción de la red en la que dos nodos pueden colisionar. Dos nodos de la red pertenecen al mismo dominio de colisión si sus tramas pueden interferir entre sí. Dominio de colisión es, por tanto, un subconjunto físico de la red en donde es posible que las tramas de red de un nodo puedan colisionar o interferir con las de otro, provocando la necesidad de retransmisiones y una pérdida del rendimiento de la red.

Conmutador inalámbrico. Dispositivo especial de la red, normalmente un *switch* de características avanzadas, que permite la gestión centralizada de todos los puntos de acceso de una instalación inalámbrica.

Cross-connect. Operación de interconexión mediante la cual en uno de los lados se sitúan las filas de pines de conexión semejantes a los jacks RJ45, mientras que en el lado opuesto se sitúan las equivalentes filas de conectores. Sobre estos conectores se enchufan los latiguillos que no son más que cables de conexión que actúan de puente entre dos elementos de conexión.

D

Datagrama. Tipo de paquete (nivel 3 de OSI) utilizado en servicios de comunicaciones sin conexión.

Despliegue. Conjunto de acciones que permiten la instalación progresiva de un sistema distribuido de sistemas y aplicaciones.

Dirección IP. Literal numérico formado por cuatro números enteros de ocho bits cada uno, separados por un punto, y que expresa la dirección de un nodo y que lo identifica unívocamente en el nivel 3.

Dirección MAC o dirección física. Dirección lógica de una interfaz de red en el nivel 2. Se compone de 12 cifras hexadecimales.

E

Estándar. Conjunto de reglas que regulan algún aspecto de una comunicación para que los productos de distintos fabricantes logren la interoperabilidad entre ellos. Los estándares se recogen en documentos que se hacen oficiales cuando una asociación de estándares internacionales lo aprueba.

Encaminamiento o enrutamiento. Técnica por la que se evalúan y deciden las rutas disponibles para transportar un paquete de datos desde su origen en una red hasta su destino en otra red distinta.

Encapsulación de protocolo. Encapsular un protocolo A dentro de otro B es ponerle cabeceras de protocolo B a cada paquete de datos del protocolo A. Como ejemplo, podríamos decir que el transporte ferroviario de coches consiste en encapsular según las normas ferroviarias el transporte habitual por carretera. Frecuentemente se utiliza el término *tunneling* o tunelización como sinónimo de encapsulación de un protocolo.

Escritorio. Suele utilizarse este término por el conjunto de aplicaciones clientes que puede ejecutar el usuario desde su ordenador cliente.

F

Falso positivo. Son las alarmas registradas en el sistema que proceden de situaciones que no son de riesgo, pero que por error son evaluadas por el sistema de alarmas como de cierto peligro.

Filtro, aplicado a una conexión. Consiste en la evaluación del tráfico de una conexión o de alguno de sus parámetros por comparación con un patrón de referencia que la permite o la impide. A este patrón se le denomina directiva del filtro.

G

GPL o Licencia Pública General GNU. Licencia creada por la *Free Software Fundation* orientada a proteger la libre distribución, modificación y uso de software. Es la licencia usada para las distribuciones de sistemas GNU/Linux.

H

Hacker. Neologismo que designa a la persona que está en la cúspide de conocimiento de una profesión informática. Los hackers no son piratas. Cuando un hacker roba información o asalta equipos o redes se convierte en un dañino cracker. Las leyes de los distintos países legislan como delito algunas de las actuaciones de crackers, que quedan penalizadas por la ley.

Host o nodo. Ordenador con capacidad de interactuar en red o capaz de alojar algún tipo de servicio de red. Por extensión, nodo en Telemática suele atribuirse a cualquier dispositivo activo conectado a una red. El término host suele asociarse a un nodo que aloja un servicio de red y que es proporcionado a los clientes a través de la red a la que se conecta, por ello, un host siempre es un nodo. Por ejemplo, son nodos las estaciones cliente, los servidores, los encaminadores, etc.

Hot spot. Punto de acceso público al que los clientes inalámbricos se pueden conectar bajo ciertas restricciones como el pago previo del servicio, aunque también puede ser gratuito. Es una instalación muy típica de lugares públicos como aeropuertos, recintos feriales, hoteles, etc.

I

Instalación en cascada. Se dice que un conjunto de dispositivos están instalados en cascada o de modo jerárquico cuando unos están conectados a los otros de modo que la salida de uno es la entrada de otro.

Interoperabilidad. Se dice que dos equipos son interoperables cuando construidos con distinta tecnología o perteneciendo a diferentes fabricantes son funcionalmente compatibles entre sí.

L

LAN *(Local Area Network)* o red de área local. Es una red geográficamente reducida con una baja tasa de error y comunicaciones de alta velocidad.

M

MAN *(Metropolitan Area Network)* o red de área metropolitana. Es una red geográficamente dispersa con una baja tasa de error y comunicaciones de media-alta velocidad, ampliamente utilizada para la distribución de TV, acceso a Internet y telefonía móvil.

N

Nivel de atenuación. Se mide en decibelios (dB) e indica una medida de las pérdidas de señal a lo largo del cable. Así, una pérdida de 10 dB indica que la energía de la señal transmitida es 10 veces menor a la salida que a la entrada, una pérdida de 20 dB supone que la energía de salida es un uno por ciento de la entrada, 30 dB implica un uno por mil de la entrada, etc.

O

***Outsourcing* o externalización.** Las grandes empresas suelen tener un departamento especializado en el soporte de los usuarios, pero en las pequeñas compañías suele ser el departamento de informática el que se encarga también de proporcionar soporte a los usuarios de la red. Existe una tendencia actual a externalizar (así es como se llama en la jerga empresarial) el soporte a los usuarios contratando a otras empresas que lo hagan en su nombre: se trata de un nuevo servicio de *outsourcing*.

P

Paquete. Bloque de datos propio del nivel de red (nivel 3 de OSI).

Parche. Actualización que afecta a una parte de un sistema operativo y que corrige algún error, tapa algún agujero de seguridad, introduce alguna mejora o implementa una nueva funcionalidad.

***Plug & Play* o «enchufar y listo».** Tecnología que han incorporado muchos fabricantes de dispositivos que facilitan la labor de configuración a los usuarios al conseguir que los parámetros necesarios se asignen de modo automático evitando colisiones entre los distintos dispositivos de hardware. Un ejemplo usual de dispositivo *plug & play* es el pendrive que se conecta al puerto USB de un PC.

Protocolo. Conjunto de reglas perfectamente organizadas que dos ordenadores deben seguir, y que por tanto comparten, para que puedan entenderse. Son reglas convenidas de mutuo acuerdo entre los participantes en una comunicación, cuya misión es regular algún aspecto de esta.

Publicar una aplicación. El nombre técnico para asegurar la accesibilidad de las aplicaciones web es «publicar» la aplicación. Obviamente, antes de esta publicación se deberá proceder a la instalación de las aplicaciones y ficheros necesarios que den soporte a la aplicación web.

Punto de acceso inalámbrico o AP *(Access Point).* Es el dispositivo que centraliza las comunicaciones inalámbricas y que suele hacer de integrador entre la red cableada y la red inalámbrica.

R

RAEE o Residuos de Aparatos Eléctricos y Electrónicos. Son los aparatos eléctricos o electrónicos, o sus componentes, al final de su vida útil. Se considera un aparato eléctrico o electrónico todo aquel que para funcionar necesite corriente eléctrica o campos electromagnéticos, y se utiliza con una tensión nominal no superior a 1 000 voltios en corriente alterna y 1 500 voltios en corriente continua, además de los aparatos necesarios para generar, transmitir y medir tales corrientes y campos.

Red cableada. Aquella red en la que las transmisiones físicas de los mensajes de la red se realizan a través de medios guiados: cables metálicos o de fibra óptica.

Red cliente-servidor. Aquella en que los ordenadores de la red tienen una función específica como cliente o como servidor, pero no como ambos a la vez.

Red entre iguales *(peer-to-peer)* o p2p. Red en la que todos los nodos se comportan como clientes y servidores simultáneamente de modo que cualquier servicio es brindado a la red directamente al cliente que lo solicita sin necesidad de intermediarios.

Red inalámbrica. Red en la que las señales transmitidas que son ondas de radio utilizan el espacio vacío o atmosférico como medio de transmisión, sin que sean necesarios tendidos de cableado.

Red perimetral. Es la red formada por todos los nodos de una red que pueden mantener comunicaciones hacia la red interna y hacia la red externa, por lo que suelen estar situados en la frontera entre ambas redes. En la documentación técnica es frecuente referirse a las zonas desmilitarizadas como redes perimetrales o, de modo más simple, red de perímetro. Así, para expresar que un servidor está situado en una DMZ podremos decir que es un servidor del perímetro.

Roaming. Significa «itinerancia» y es la función de los sistemas inalámbricos formados por varias celdas por las que un cliente que se desplaza cambia de celda en celda, buscando la mejor cobertura, sin perder la conexión a la troncal de la red a la que se conectan todas las celdas.

RFC o *Request For Comments.* Conjunto de comentarios sobre Internet que comenzaron a publicarse en los albores de Internet (originalmente ARPANET) en 1969 y que recogen propuestas de estandarización de protocolos de red. Se pueden encontrar en **www.ietf.org** o en **www.rfc-editor.org.**

S

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

SAN. Red especializada en conectar virtualmente un conjunto de discos a los servidores que los utilizarán empleando tecnologías de alta velocidad y, frecuentemente, redundantes.

Segmento. Bloque de datos definido en el nivel de transporte (nivel 4 de OSI).

Servicio. En un sistema operativo, es una tarea que se está ejecutando en ese sistema sin necesidad de un terminal (decimos que corre en *background* o, en el mundo Linux, «que es un demonio») y que proporciona una utilidad determinada. Los clientes de ese servicio realizarán sus peticiones al servicio a través de los procedimientos de comunicación soportados por el sistema operativo.

Servidor proxy. Un servidor proxy de un servicio es un intermediario de red entre el cliente que solicita el servicio y el servidor que lo brinda. El cliente solicita el servicio al proxy quien a su vez gestiona la petición en su propio nombre al servidor de destino.

System crash. Fallo irrecuperable del sistema operativo provocado por un problema importante en el hardware o por un mal funcionamiento del software del sistema. En Windows, se puede detectar un *system crash* cuando aparece inesperadamente una pantalla azul llena de mensajes indescifrables que proporcionan alguna información sobre la causa del error a los ingenieros de sistemas. En el argot profesional a esta pantalla se la denomina BSOD (*Blue Screen Of Death,* Pantalla azul de la muerte) en Windows o Kernel panic en Linux.

T

Tasa de error. En una transmisión es la proporción entre los bits erróneos y los bits totales transmitidos. En la jerga profesional, cuando la tasa de error de una transmisión se dispara, se dice que la «línea tiene ruido».

Teleinformática o Telemática. Técnica que trata de la comunicación remota entre procesos. Para ello, debe ocuparse tanto de la interconectabilidad física, forma del conector, tipo de señal, parámetros eléctricos, etc., como de las especificaciones lógicas: protocolos de comunicación, detección y corrección de errores, etc.

Toma a tierra. En electricidad, es la conexión al nivel de referencia de cero voltios. Las instalaciones de edificios bien construidos incorporan un sistema de cableado subterráneo (picas de tierra) en contacto con el subsuelo del edificio que se toma como el nivel de cero voltios. Todos los dispositivos eléctricos o electrónicos de la instalación del edificio, entre ellos las mallas de los cables STP y las carcasas de los dispositivos de red y racks, deben estar conectados a estas picas de tierra.

Topología. Es la disposición física del sistema de cableado de una red que predispone el tipo de comunicaciones que se podrán operar en ella. Los tipos más básicos de topologías para redes locales son las estrellas, los anillos y las mallas.

Trama. Bloque de datos definido en el nivel de enlace de datos (nivel 2 de OSI). Cada trama se compone de un conjunto de campos entre los que se encuentran los campos de dirección física de origen y de destino de la trama. Cada trama también integra un campo que sirve para realizar el control de errores de la transmisión.

Transceptor o transceiver. Dispositivo con una entrada y una salida que altera la naturaleza de la señal de entrada y la pone en la salida manteniendo la información que transporta. Por ejemplo, podría entrar señal eléctrica y salir señal luminosa. Otro ejemplo de transceptor es un micrófono que recoge señales acústicas y las convierte en eléctricas. El transceptor inverso al micrófono sería el altavoz, que a partir de señales eléctricas genera a su salida señales acústicas.

U

U. Medida estandarizada de las bandejas de un rack o armario. Es la abreviatura de *Rack Unit.* Equivale a una altura en armario de 1,75 pulgadas (44,45 mm). En cada U se incluyen en las paredes del rack tres tornillos de fijación.

W

WAN *(Wide Area Network)* o red de área local extensa. Es una red geográficamente distribuida, con una alta tasa de error en sus comunicaciones y que permite enlaces remotos de moderada velocidad.

WLAN *(Wireless Local Area Network)* o red de área local inalámbrica. Red local que transmite mediante ondas de radio y ofrece dos ventajas sustanciales: no es necesario extender cableado por lugares en los que sería imposible o muy difícil y, por otra parte, admite la movilidad de los ordenadores de la red.

Ciclo Formativo Grado Medio

Redes locales

«La base de tu futuro»

Esta es la filosofía del proyecto editorial de McGraw-Hill para Ciclos Formativos, una etapa decisiva en la formación de profesionales.

El proyecto para el módulo Redes locales, incluido en el nuevo ciclo formativo Técnico en Sistemas Microinformáticos y Redes, y que está estructurado en dos niveles de uso, para el alumno y para el profesor, ha sido desarrollado según tres principios básicos:

- Una metodología basada en la práctica y en la adecuación de contenidos y procedimientos a tu realidad profesional.
- Unos materiales desarrollados para conseguir las destrezas, habilidades y resultados de aprendizaje que necesitarás para conseguir tu título y desenvolverte en el mercado laboral.
- Una presentación de los contenidos clara y atractiva, con variedad de recursos gráficos y multimedia que facilitarán tu aprendizaje.

El proyecto para el módulo profesional *Redes locales* ha sido desarrollado considerando las unidades de competencia del **Catálogo Nacional de Cualificaciones Profesionales:**

Unidades de competencia profesional
Instalar, configurar y verificar los elementos de la red local según procedimientos establecidos. **(UC0220_2)**
Monitorizar los procesos de comunicaciones de la red local. **(UC0955_2)**

Confiamos en que esta obra sea una herramienta útil y eficaz, y que contribuya a tu formación como profesional.