C.F.G.S. DESARROLLO DE APLICACIONES MULTIPLATAFORMA

MÓDULO:

Sistemas Informáticos

Unidad 9

Redes (III)-Internet

INDICE DE CONTENIDOS

1. INTRODUCCIÓN

Internet ha supuesto un cambio en la vida de las personas comparable a la Revolución Industrial del siglo XIX, revolucionado el mundo de la informática y de la comunicación como nada lo había hecho antes. La invención del telégrafo, el teléfono, la radio y el ordenador sientan las bases para esta integración sin precedentes de posibilidades que supone Internet, la cual es al mismo tiempo un medio de comunicación mundial, un mecanismo para la difusión de información y un medio para la colaboración e interacción entre individuos y sus ordenadores independientemente de su localización geográfica. Además, con Internet, el acceso a determinados recursos, principalmente información, que anteriormente estaban reservados a un grupo muy reducido de personas, se está haciendo accesible a los ciudadanos “de a pie”. Estos cambios se han visto motivados por los siguientes aspectos:

- Mejora de las comunicaciones que permiten acceder a estos recursos a cualquier usuario desde su domicilio.
- Aparición y mejora de las tecnologías que proporcionan estos recursos.
- Presentación de la información de forma fácilmente comprensible por la mayor parte de los usuarios.

Pero, ¿qué es Internet? Internet es el ejemplo más palpable del tipo de estructura que analizamos en la unidad anterior; es decir, no es más que la interconexión de multitud de redes, cada una de las cuales puede ser de un tipo distinto, donde es posible la comunicación entre cualquier equipo que se encuentre conectado a cualquiera de las redes que la constituyen. Por eso Internet es conocida también con el sobrenombre de “la red de redes”. Internet es una interred pública y de ámbito mundial, en la que los equipos utilizan la pila de protocolos TCP/IP para comunicarse.

Podemos pensar que Internet es algo muy reciente, y no andamos desencaminados. Sin embargo, aunque su explosión ha tenido lugar en la década de los noventa, sus orígenes se remontan un poco más atrás. Podemos datar la aparición de Internet en los años 60, en plena guerra fría, en el ámbito militar. En este contexto histórico de alta tensión, el gobierno estadounidense buscaba una forma de asegurar el mantenimiento de las comunicaciones entre distintos puntos vitales de la nación, para que, en el caso de un ataque nuclear ruso, se pudiese acceder a la información militar desde cualquier punto del país. Hasta ese momento todas las comunicaciones militares usaban la red telefónica pública, que se consideraba vulnerable, puesto que la destrucción de algunas de las oficinas interurbanas clave podía fragmentar el sistema en muchos trozos incomunicados. El nuevo sistema de comunicación debía de cumplir los siguientes requerimientos:

- La eliminación de cualquier "autoridad central", ya que sería el primer blanco en caso de un ataque; en este sentido, se pensó en una red descentralizada y diseñada para operar en situaciones difíciles.

- Cada máquina conectada debería tener el mismo estatus y la misma capacidad para mandar y recibir información.
- El envío de los datos debería descansar en un mecanismo que pudiera manejar la destrucción parcial de la Red.
- Lo importante no debía ser la ruta que siguiese la información desde el origen al destino, sino que ésta llegara a su destino.

Ante esta situación y con estas premisas, **la Agencia de Proyectos de Investigación Avanzada de Defensa** (**DARPA** – Defensa Advanced Research Projetcts Agency) de Estados Unidos construye en 1969 la **red ARPANET**, una red de comunicaciones en la que los mensajes se dividían en pequeñas unidades de información, cada una de las cuales contenía la dirección de destino pero sin especificar una ruta específica para su tránsito por la red; por el contrario, cada una de ellas buscaba, de forma independiente, la manera de llegar al destinatario por alguna de las rutas disponibles. Si bien en 1969 la red ARPANET estaba formada por sólo 4 ordenadores, otros muchos fueron añadiéndose paulatinamente a la estructura durante los siguientes años, y no todos ellos del ámbito militar, sino también del ámbito académico. Durante la década de 1970 habían surgido varios protocolos para su uso en ARPANET; sin embargo, dichos protocolos no eran compatibles, por lo que la interconexión de redes era muy difícil y, por tanto, el intercambio de información muy complicado. Debido a ello, DARPA encargó y proporcionó fondos para la investigación y desarrollo de nuevos protocolos que se utilizarían en dicho sistema de comunicaciones, los cuales deberían permitir la interconexión sencilla de redes heterogéneas. Este proceso culminó con la invención del modelo y pila de protocolos TCP/IP, al que se migró finalmente en enero de 1983. En este mismo año de 1983 la motivación de ARPENET se vuelve exclusivamente científica y académica, cuando se produce la separación de su segmento militar, el cual decide construir su propia red independiente, llamada MILNET.

En 1984 la Fundación Nacional para las Ciencias de Estados Unidos, NFS, viendo las posibilidades que ofrecía una red como ARPANET y viendo su enorme impacto, se lanzó a la construcción de una red similar que pudiera estar abierta a todos los grupos de investigación de las universidades. Para ello conectó primeramente en una red troncal sus seis centros de superordenadores situados en San Diego, Boulder, Champaign, Pittsburgh, Ithaca y Princeton. Posteriormente, a esta red troncal se conectaron otras redes regionales para que los usuarios de miles de universidades, laboratorios de investigación, museos y bibliotecas tuvieran acceso a cualquiera de los superordenadores y se comunicaran entre sí. A todo este sistema formado por la red troncal y las redes regionales, se le llamó red NSFNET. El crecimiento exponencial que experimentó NSFNET, así como el incremento continuo de su capacidad de transmisión de datos, determinó que la mayoría de los miembros de ARPANET terminaran conectándose a esta nueva red y, en 1989, ARPANET se declara disuelta.

Durante la década de 1990, muchos otros países también construyeron redes nacionales de investigación, con frecuencia siguiendo el patrón de ARPANET y NFSNET. Éstas incluían, por

ejemplo, a EuropaNET y EBONE en Europa. En la prehistoria de la red en España está la creación, el año 1988, por el Plan Nacional de Investigación y Desarrollo, de un programa para la Interconexión de los Recursos InformáticoS (IRIS) de los centros de investigación. Al principio lo gestionó Fundesco (fundación de Telefónica). La RedIRIS, que desde enero de 1994 está gestionada por el Consejo Superior de Investigaciones Científicas, fue el motor de conexión de ordenadores y formación de personas, y de ella surgieron muchas de las primeras iniciativas de redes que se produjeron en nuestro país. Con la interconexión de todas estas redes con NFSNET, nace la red mundial de comunicaciones que hoy conocemos con el nombre de red INTERNET.

Entre 1970 y 1990, Internet y sus predecesores tenían cuatro aplicaciones principales:

- **El correo electrónico** - Que proporciona capacidad a los usuarios de la Red para redactar, enviar y recibir mensajes.
- **Las noticias** - Que son foros especializados en los que los usuarios con un interés común pueden intercambiar mensajes.
- **Inicio remoto de sesión** - Que permite a los usuarios a que puedan iniciar una sesión en cualquier otro ordenador en el que tengan una cuenta de usuario.
- **Transferencia de archivos** - Que permite a los usuarios la copia de archivos de una máquina a otra.

Hasta principios de la década de 1990, Internet era una red sólo apta para investigadores y técnicos, debido a la alta complejidad del uso de la misma, lo cual impedía su apertura al público general. En 1992 una nueva aplicación, la World Wide Web o telaraña mundial cambió todo esto, atrayendo a millones de nuevos usuarios no académicos a la red. La World Wide Web permite un acceso sencillo y comprensible a la información disponible en Internet y que esté almacenada en forma de páginas electrónicas o páginas Web, las cuales pueden contener texto, imagen, sonido y vídeo, y pudiendo combinar todos estos elementos dentro de las mismas. La Web es un método muy atractivo y completo para transmitir y presentar la información, lo cual la hace accesible a cualquier usuario independientemente de su grado de conocimiento técnico.

A lo largo de la unidad profundizaremos un poco en el funcionamiento de cada uno de los servicios o aplicaciones principales de Internet mencionados.

1. ASIGNACIÓN DE DIRECCIONES IP Y NOMBRES DE DOMINIO

En una interred sin comunicación con el exterior, su propietario puede establecer para sus redes interconectadas y para sus equipos las direcciones IP que desee, siempre y cuando no haya dos equipos con la misma dirección, evidentemente. Sin embargo, en una interred pública como Internet no puede permitirse que cada uno asigne a su red el identificador de red que

desee, no puede permitirse una asignación desordenada de direcciones, porque esto nos llevaría a una duplicidad de direcciones que haría imposible el enrutamiento. Para evitarlo, en Internet tiene que haber un organismo que es el que controla y gestiona la asignación de direcciones:

- Hasta 1998 dicho organismo era el **IANA** (Internet Assigned Number Authority) o **Autoridad para la asignación de direcciones IP**.
- Posteriormente dicha labor pasó a manos del **ICANN** (Internet Corporation for Assigned Names and Numbers) u **Organización de Internet para la asignación de direcciones IP y nombres de dominio**.

No obstante, debido a las dimensiones y al carácter mundial que ha adquirido Internet, la gestión y asignación de los recursos se han delegado en ciertas autoridades regionales, llamados **RIRs** (Regional Internet Registries) o **Registros Regionales de Internet**, encargándose el ICANN de las tareas de coordinación entre ellos. Así, el ICANN ha asignado grandes bloques de direcciones IP a cada uno de los distintos RIRs, los cuales se encargan de su reparto real dentro de la región que administran. Actualmente hay cinco Registros Regionales de Internet:

- **AfriNIC** - que se encarga de la región formada por **África**.
- **APNIC** - que se encarga de la región formada por el **Pacífico Asiático**.
- **ARIN** - que se encarga de la región formada por **Norteamérica**.
- **LACNIC** - que se encarga de la región formada por **Latinoamérica y El Caribe**.
- **RIPE NCC** - que se encarga de la región formada por **Europa, Oriente Medio y parte de Asia Central**.

2. REDES PRIVADAS - PROTOCOLO NAT

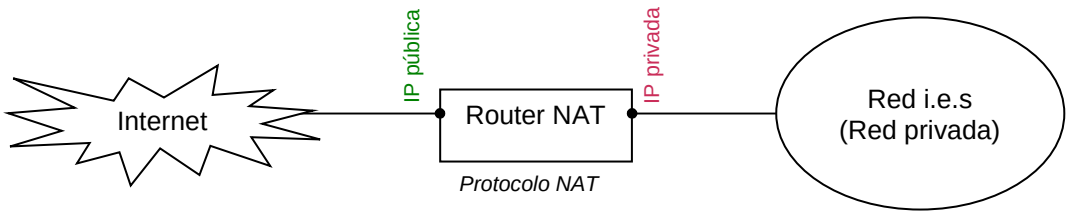
Para conectar una red privada a Internet se utiliza un router provisto de un protocolo especial: **el protocolo NAT**, Network Address Translation o **traducción de direcciones de red**. Este router, que recibe asimismo el nombre de router NAT:

- Estará conectado tanto a Internet como a la interred privada. Con lo cual, tendrá una dirección IP de Internet (IP pública), y una dirección IP dentro de la red privada (IP privada).
- Será el router de salida a Internet de toda la interred privada. Es decir, será el router que conectará la interred privada con Internet.
- Será el único equipo que existe para el resto de Internet. El resto de equipos de la red privada no serán visibles desde Internet, será como si no existiesen.
- Será el representante de cara a Internet de todos los equipos de la red privada. Cuando un equipo de la red privada quiere conectarse a un equipo de Internet, el

router NAT lo hará por él, de tal manera que será el router NAT el que se conecte a la máquina destino de Internet, para posteriormente reenviar las respuestas que ésta le mande al ordenador original de la red privada. La máquina de Internet que recibe la conexión lo hace desde la dirección pública del router NAT y no sabe nada de la existencia de una red privada detrás del router.

- Su conexión a Internet será compartida por todos los equipos de la red privada.

EJEMPLO



EJEMPLO

Imagina que le has dejado instrucciones al secretario o secretaria de tu oficina de que no te pase ninguna llamada a no ser que así se lo indiques. Más tarde realizas una llamada a un cliente potencial al cual le dejas un mensaje de que te devuelva la llamada, y avisas a tu secretario o secretaria de que estás esperando una llamada del cliente y de que te la pase cuando ésta se produzca. Cuando el cliente llame, lo hará al teléfono principal de la oficina, el de secretaría, pues es el único número de teléfono que el cliente conoce, el único aparato con un número de teléfono público. Entonces el cliente le dirá al secretario o secretaria que desea hablar contigo y, para poder pasarte la llamada, tendrá que averiguar cuál es la extensión de teléfono que tienes asociada en la oficina, mirando, por ejemplo, en una hoja en la que tiene una tabla con las correspondencias despacho-extensión. Pues bien, de manera semejante, en el caso de nuestra red privada, el router NAT haría las funciones del secretario o secretaria del ejemplo.

El proceso que se lleva a cabo en nuestra red privada cuando un equipo de la red privada quiere conectarse a un equipo de Internet es el siguiente:

- El equipo de la red privada lanza la conexión al ordenador de Internet como lo haría en cualquier otra situación. Es decir, los paquetes IP tendrán como dirección IP de origen la del equipo de la red privada y como dirección IP de destino la del ordenador de Internet al que se quiere conectar.
- Este tráfico, para salir de la interred privada tiene que pasar por el router NAT, pues es el que da conectividad hacia Internet.

- El router sustituirá entonces la dirección IP de origen de los paquetes por su dirección IP pública. Por lo tanto, será el router NAT el que se conecte a la máquina destino de Internet. De hecho, la máquina de Internet que recibe la conexión lo hace desde la dirección pública del router NAT y no sabe nada de la existencia de una red privada detrás del router.
- El ordenador de Internet que recibe la conexión dirigirá el tráfico de respuesta al router NAT, pues es el que ha establecido la comunicación con él a todos los efectos.
- Evidentemente, el router NAT tiene la información y los mecanismos necesarios para saber a qué equipo interno de la red privada está representando en cada comunicación abierta y poder así redirigirles este tráfico de respuesta.

3. CONEXIÓN A INTERNET

Si la conexión a Internet se realiza para leer el correo, navegar y chatear, no se necesita una gran velocidad entonces le basta con unos 56 Kbps que suministra un módem sencillo a través de la línea telefónica. Además, si esta conexión va a realizarse durante varias horas diarias, lo que necesita es una tarifa plana que le supondrá un ahorro importante. Pero si lo que pretende es bajar archivos de música o películas, lo que se necesita es una banda ancha de 512 Kbps o 1 Mbps como una línea ADSL que además permite conexión permanente 24 horas al día sin coste adicional y por supuesto una navegación mucho más rápida con intercambio de archivos mucho más fiable. Claro que estas diferencias de velocidad llevan asociada una importante diferencia de precio. También existe la conexión por cable con unas prestaciones similares al ADSL.

En el apartado anterior vimos que en los inicios de la red Internet, para conectar nuestra red a la misma, debíamos solicitar primero a un organismo llamado ICANN que nos otorgase la propiedad de un identificador de red y nos proporcionara la conexión a la infraestructura de interred existente. En España, algunas instituciones públicas importantes como universidades, consejerías, ministerios, etc. así lo hicieron y tienen conexión directa a Internet de esta forma. Sin embargo, este caso ya no es la norma, sino más bien la excepción, y la situación que nos encontramos actualmente en el 99% de los casos es la de disponer de una conexión a Internet facilitada por un **ISP (Internet Service Provider) o Proveedor de Servicios y Acceso a Internet**.

Un proveedor de servicios y acceso a Internet no es más que una empresa que proporciona acceso a Internet a sus clientes, ya sean empresas o particulares, a cambio del pago de una cuota mensual.

Ya sabemos que, como usuarios finales, para contratar una conexión a Internet tenemos que hacerlo a través de un **ISP**. Ahora bien, ¿qué proveedor de acceso a Internet elijo? Si tenemos la posibilidad de elegir entre varios proveedores de servicios, lo cual no es posible en todos los lugares de la geografía española, haremos nuestra elección atendiendo principalmente a dos criterios básicos:

- **Velocidad de la conexión** - La velocidad de conexión hace referencia a la cantidad de información que puede ser transmitida por unidad de tiempo en el tramo de la conexión entre el usuario final y su proveedor de acceso a Internet. Dicha velocidad se mide generalmente en Kilobits por segundo (Kbps) o Megabits por segundo (Mbps) y está estrechamente relacionada con la tecnología que utiliza el proveedor de servicios en su red de acceso. Además, en la mayoría de las ocasiones dicha velocidad es asimétrica; es decir, la velocidad de subida es distinta a la velocidad de bajada.
- **Precio de la conexión** - Como es normal en una economía de mercado, el precio de la conexión a Internet debe variar de un proveedor a otro, por lo que hacer una buena elección es importante y puede ahorrarnos bastante dinero. No obstante, el precio de una conexión dependerá fundamentalmente de la velocidad de conexión que se contrate. Además, a la hora de escoger proveedor, también es interesante saber si tenemos la posibilidad de acogernos a una tarifa plana o no y si dicho modelo de contrato nos interesa, o también si el proveedor de acceso a Internet limita o no el volumen de descarga.

3.1. TIPOS DE CONEXIONES A INTERNET

Las tecnologías de conexión más utilizadas en las redes de acceso son las siguientes:

3.1.1. CONEXIÓN A TRAVÉS DE LA RED TELEFÓNICA CONMUTADA

También llamada **dial-up**, es el método de conexión más antiguo y era el único utilizado cuando internet daba sus primeros pasos. El acceso es realizado por el usuario mediante un módem y una línea telefónica convencional. Este tipo de conexión es cada vez menos usada, ya que la capacidad de transmisión de datos no supera los 56 kbps, lo que hace que la navegación sea muy lenta. Con la popularización de los servicios de acceso de banda ancha y sus precios muy accesibles, el acceso dial-up está prácticamente en extinción.

Además de la baja velocidad, la conexión por línea telefónica **no es estable y mantiene la línea telefónica ocupada cuando se conecta a internet.** O sea, que se navega por internet o se habla por teléfono. Sin importar el horario en que se acceda a internet, los gastos de la cuenta telefónica pueden aumentar considerablemente.

La conexión a través de la Red Telefónica Conmutada (RTC), también llamada Red Telefónica Básica (RTB):

- Ha sido el tipo de conexión más común entre los primeros usuarios de Internet, pues el teléfono estaba y está presente en la mayoría de hogares y empresas y, por lo tanto, al utilizar como red de acceso una infraestructura ya existente, la inversión para su puesta en funcionamiento era escasa.
- Sin embargo, se trata de una tecnología lenta, de velocidad asimétrica, pues proporciona una velocidad teórica máxima de bajada de 56 Kbps, y una velocidad

teórica máxima de subida de 33’6 Kbps, aunque éstas suelen ser siempre algo menores.

- La Red Telefónica Básica hace uso del par de cobre como medio de transmisión entre el usuario final y la central del ISP.
- El acceso a Internet a través de la Red Telefónica Conmutada es conocido con el sobrenombre de conexión dial-up, pues la conexión no es permanente, sino que se establece en el instante mediante una llamada telefónica al número proporcionado por el ISP. Asimismo, la conexión desaparece al terminar.
- Además, dicha red es analógica, por lo que los datos, al ser digitales, deberán ser transformados para poder ser transmitidos por la red, tarea de la cual se encarga un periférico llamado módem.

3.1.2. CONEXIÓN xDSL

La conexión xDSL es suministrada por medio de la red telefónica convencional, pero es difiere al acceso dial-up. Un módem convierte la información en una señal eléctrica que la transforma en una frecuencia diferente a la utilizada para la voz, de esta manera una señal no interfiere en el uso del teléfono. Esto quiere decir que se puede navegar por internet y utilizar el teléfono al mismo tiempo. Sin embargo, es bueno recordar que es necesario que la PC tenga una placa de red Ethernet.

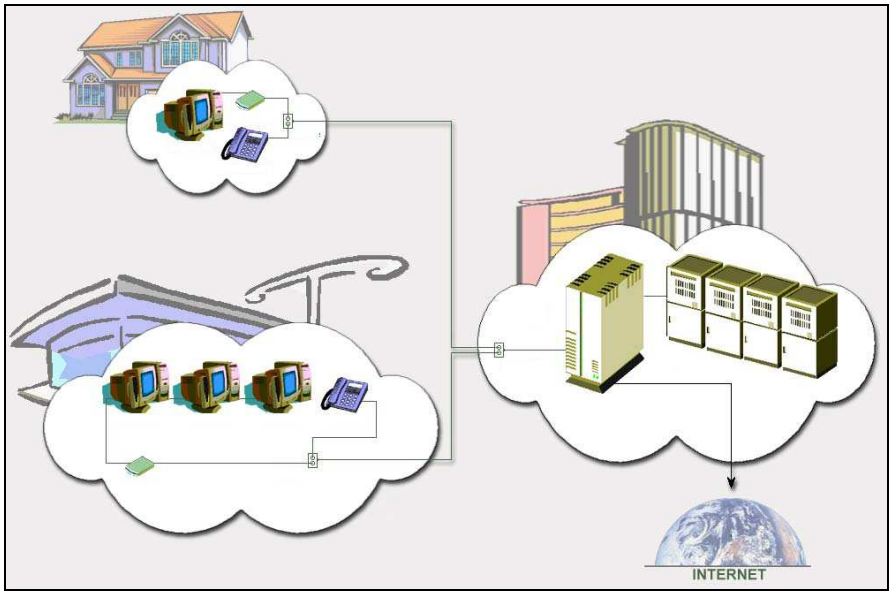
El servicio xDSL funciona mediante la contratación de un proveedor de acceso, al igual que el dial-up, y es posible acceder a servicios con diversas velocidades. Por ejemplo, en el ADSL, la velocidad varía de 256 kbps a 8 mbps; en el ADSL2 o ADSL2+ va desde 256 kbps hasta 24 Mbps; en el VDSL puede llegar a una velocidad de 52 Mbps y en el VDSL2 hasta 100 Mbps. A pesar de la popularidad de ese tipo de acceso, no está disponible en todos lados.

El xDLS tiene como desventaja que, al tratarse de un servicio compartido, la navegación puede ser más lenta en horarios pico, cuando muchos usuarios utilizan el servicio simultáneamente.

La conexión mediante la tecnología ADSL (Asymmetric Digital Subscriber Line) o Línea de Abonado Digital Asimétrica:

- Es una tecnología de acceso de las llamadas de banda ancha o de alta velocidad, capaz de proporcionar velocidades de conexión de varios Mbps. Además, dicha velocidad es asimétrica; es decir, es distinta la velocidad de bajada que la de subida.
- Utiliza el mismo cableado de par de cobre del teléfono analógico para la transmisión de datos a alta velocidad, haciendo uso de una nueva técnica distinta de la usada para la transmisión de la voz, de tal manera que ambas no se interfieren y pueden llevarse a cabo de manera simultánea. Es decir, que se puede estar usando el teléfono al mismo tiempo que se está conectado a Internet mediante ADSL.
- Además, se trata de una conexión permanente; es decir, la conexión está siempre activa y no hace falta su establecimiento mediante una llamada.

- Utiliza para la transmisión a través del medio un periférico llamado módem ADSL.
- Es probablemente la tecnología de alta velocidad para el acceso a Internet que más aceptación está teniendo entre los usuarios finales. Sin embargo, no todas las líneas telefónicas pueden ofrecer este servicio, debido a que las exigencias de calidad del par de cobre, tanto de ruido como de atenuación, por distancia a la central, son más estrictas que para el servicio telefónico básico.



3.1.3. CONEXIÓN POR CABLE

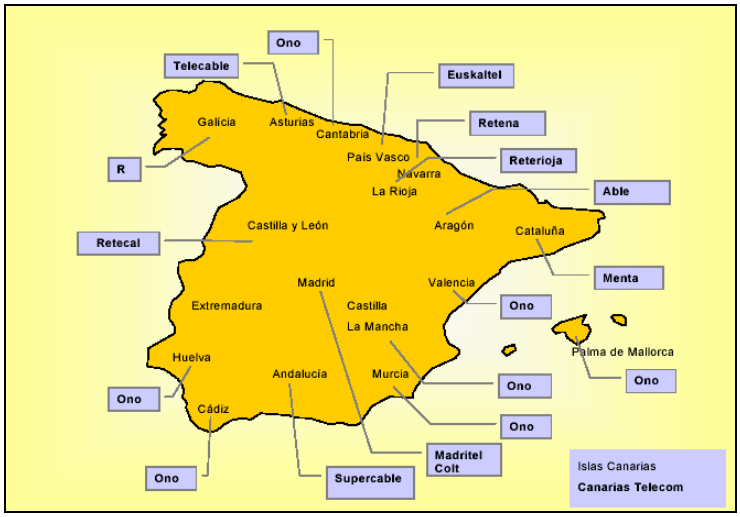
La conexión por cable es cada vez más popular y utiliza la misma infraestructura que la del servicio de cable contratado, lo que facilita la instalación. Muchos servicios de televisión por cable ofrecen en el paquete el acceso a internet con distintas velocidades. En sólo un cable se transfieren el servicio de televisión y los datos de internet. Un aparato llamado **splitter** separa la señal de cable de la de los datos web, y un cable conectado a un módem permite el acceso a internet.

Una de las ventajas de ese tipo de conexión, es que tan solo basta con conectar el cable del modem a la computadora para tener conexión, sin la necesidad de marcar o activar un servicio. Para que todo eso funcione es necesario tener una placa Ethernet instalada. Este tipo de acceso sólo es posible en regiones donde existen servicios de televisión por cable.

Este tipo de acceso pone a disposición distintos tipos de velocidades. La velocidad de navegación, y el límite de las descargas y de los datos subidos, dependen del paquete que se contrate. Además, la velocidad no se ve afectada por la cantidad de usuarios u horarios en que se use el servicio. A diferencia del acceso xDSL, el usuario siempre tendrá la misma velocidad de acceso, en cualquier horario.

Esta tecnología:

- Utiliza la infraestructura de la Televisión por Cable (CATV) para proporcionar conexión a Internet utilizando el ancho de banda que ésta no utiliza.
- Utiliza una red de las llamadas híbridas, pues está compuesta por dos medios de transmisión distintos: fibra óptica en el corazón de la red, y cable coaxial en el tramo final que llega a nuestras casas.
- Forma parte del elenco de tecnologías de acceso de alta velocidad o banda ancha, ofreciendo velocidades de conexión de varios Mbps. Además, dicha velocidad es asimétrica; es decir, es distinta la velocidad de bajada que la de subida.
- Está siempre activa y no hace falta su establecimiento mediante una llamada; es decir, se trata de una conexión permanente que puede ser utilizada en cualquier momento sin necesidad de hacer nada previo más que encender el ordenador.
- Utiliza para la transmisión a través del medio un periférico llamado cablemódem o módem de cable.
- Tiene como principal freno a su expansión que es necesario desplegar una red de acceso completamente nueva, lo que supone una fuerte inversión inicial por parte de los operadores de cable, mientras que otras tecnologías, como ADSL, utilizan una infraestructura de acceso ya existente y que llega a todos los hogares, como es la red telefónica. No obstante, poco a poco, los operadores están cableando las distintas ciudades en las que operan y están extendiendo sus radios de acción o cobertura.



3.1.4. CONEXIÓN POR SATÉLITE

Otra alternativa, es la **conexión por satélite**, para la cual se necesitan equipos específicos que suelen tener un costo muy elevado. Es preciso adquirir una antena capaz de captar la señal del satélite y lo transmita a la computadora que cuente con un módem receptor interno o externo.

En algunos casos, la antena es suministrada por el propio proveedor del servicio. **Este tipo de acceso a internet, cuenta con planes que ofrecen velocidades que varían desde los 512 kbs hasta los 2 Mbps.**

Una de las ventajas de la conexión por satélite es que el acceso no depende de la localización. De esta manera se tendrá acceso a internet en cualquier lugar donde llegue la cobertura. **Sin embargo, mientras más remoto sea el lugar donde nos encontremos, más potente será la señal.**

3.1.5. CONEXIÓN POR RADIO (CONEXIONES INALÁMBRICAS)

El acceso a internet por radio es una manera de extender una conexión de banda ancha a algún lugar donde no se dispone del servicio. Ese punto puede ser desde una pequeña área restringida, como una oficina, hasta una ciudad completa. **Para eso es necesario configurar una red sin cables.** Están incluidos en esta modalidad el **Wi-fi** y el Wi-Max.

Una de las ventajas de la conexión por radio es la posibilidad de repartir el acceso y la garantía de la movilidad a los usuarios. La infraestructura básica exige un punto de entrega de servicio de internet, que puede ser un acceso por cable, xDSL o satélite, un módem compatible con el servicio, un Access Point (especie de radio) y computadoras con receptor o adaptador de red inalámbrica para captar la señal. **Al compartir una conexión de gran capacidad, los usuarios pueden dividir los gastos, al mismo tiempo, que el servicio les garantiza una conexión permanente y de bajo costo de instalación y mantenimiento**. Sin embargo, el uso simultáneo para las descargas puede perjudicar el acceso.

3.1.6. CONEXIONES MÓVILES A TRAVÉS DE TELEFONÍA: CONEXIONES 3G Y 4G

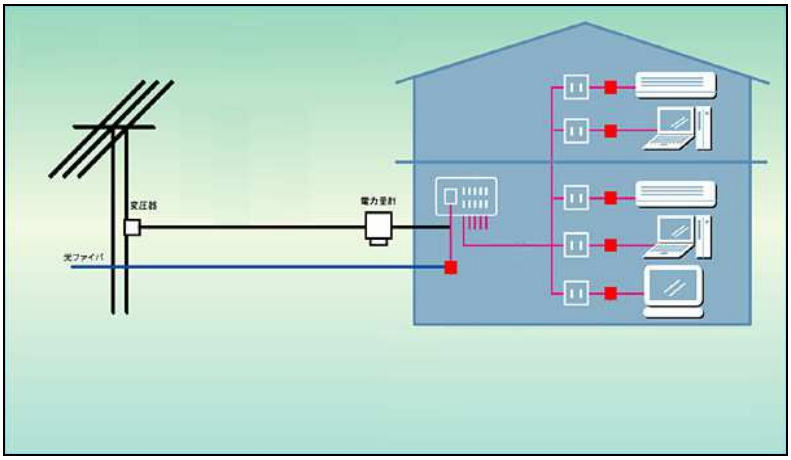
La conexión a internet a través de los teléfonos celulares es cada vez mejor. La llegada de la tecnología 3G proporcionó banda ancha a los teléfonos celulares, y otorgó una velocidad de navegación con una considerable aceleración. Sin embargo, la máxima expresión, por lo menos hasta hoy, es la aparición en el mercado del estándar 4G, el cual permite recibir y enviar datos a velocidades antes imposibles de alcanzar, lo que nos brinda la posibilidad de ver videos en calidad HD y escuchar música directamente desde la nube, entre otros.

La movilidad es una gran ventaja de los servicios de este tipo. En el caso de las redes GSM, la velocidad de transferencia puede alcanzar los 800 kbps. **En el caso de las redes CDMA, la transferencia puede llegar a alcanzar una velocidad de hasta 2 Mbps**. Estos números son ampliamente superados cuando nuestro teléfono es compatible con 3G o 4G, que pueden superar ampliamente estas cifras, alcanzando en el caso de 3G hasta los 2 Mbps, y en el caso de 4G hasta los 200 Mbps.

3.1.7. ONEXIÓN A TRAVÉS DE LA RED ELÉCTRICA. PLC

Sin lugar a dudas**, la tecnología PLC (Power Line Communications) es una de las más interesantes formas de conexión que se mencionan** ya que aprovecha las líneas eléctricas para transmitir datos a alta velocidad.

En la actualidad es uno de los sistemas alternativos de conexión más utilizados por usuarios en todo el mundo, ya que entre muchos de los beneficios que ofrece, se encuentra la posibilidad de usar el cableado eléctrico de cualquier casa para intercambiar datos entre los nodos de una red local, **con la conveniencia de no tener que invertir en el cablerío necesario para montarla,** algo que agradecen muchos hogares y pequeñas empresas.



4. PROTOCOLOS DE INFRAESTRUCTURA TCP/IP

Establecer una dirección IP diferente para cada ordenador no es tarea fácil, hay que ser muy cuidadoso y ordenado de modo que no se produzcan duplicidad de direcciones y por tanto ambigüedad en los destinos. Por eso existen mecanismos automáticos como **DHCP que asignan automáticamente la dirección a cada ordenador de la Red**. Además, un individuo normal tiene problemas a la hora de recordar direcciones compuestas por cuatro números, para facilitar esta tarea a los usuarios de Internet se ha habilitado el **DNS, un sistema mediante el cual se asocia un nombre a cada dirección IP de Internet**, lo que significa que sólo hay que recordar el nombre para acceder a un determinado dominio.

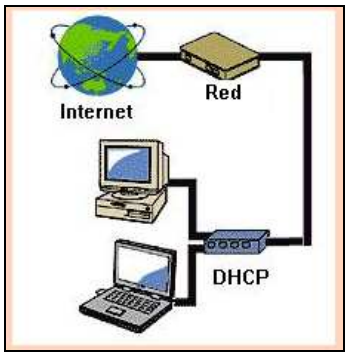
Una vez que se dispone de conexión a Internet, ya sea con un ISP u otro, ya sea con un operador u otro, ya sea usando una u otra tecnología, se puede empezar a disfrutar de las posibilidades de comunicación, acceso a información y ocio que nos ofrece la red de redes. No obstante, olvidémonos un tanto de la visión superficial que tenemos de Internet como usuarios y analicemos lo que sucede por debajo como informáticos que somos o aspiramos a ser.

No debemos perder de vista que lo que hacemos cuando usamos Internet, al igual que en cualquier otra red, es establecer procesos de comunicación. Además, estos procesos de comunicación se producen entre dos aplicaciones, estando cada una de ellas en ordenadores distintos. Ya sabemos que estas aplicaciones se comunican siguiendo una serie de reglas que vendrán especificadas en lo que se conoce en el modelo TCP/IP como protocolos de nivel de aplicación. Evidentemente, hay infinidad de protocolos de nivel de aplicación, cada uno de los cuales describe la comunicación de un determinado tipo entre dos aplicaciones de red.

Sin embargo, **dentro de los protocolos de nivel de aplicación existen unos cuantos que no tienen como finalidad definir la comunicación entre dos aplicaciones de usuario, sino que son protocolos que facilitan a los usuarios el uso de la red. Estos protocolos reciben el nombre de protocolos de infraestructura TCP/IP**, y en los siguientes apartados vamos a analizar brevemente los dos más importantes: el protocolo o servicio **DHCP** y el protocolo o servicio **DNS**.

4.1. SERVICIO DHCP

Como ya sabemos, todo equipo conectado en red tiene que tener asignada una dirección IP. Imagina que eres el administrador de una red con cientos o miles de ordenadores. ¿Te gustaría tener que ir ordenador a ordenador asignándole manualmente la dirección IP y configurándole el resto de parámetros de la red? Pero vayamos más allá, piensa que después de invertir días configurando la red en todos los ordenadores tuvieses que introducir algún cambio en dicha configuración, cosa que suele ser bastante frecuente. Tendrías entonces que ir nuevamente ordenador a ordenador modificando la configuración de los mismos. Afortunadamente, viendo el enorme esfuerzo que conllevaba esta configuración manual inicial, así como su mantenimiento, cuando se trataba de redes grandes, se ideó un **protocolo de nivel de aplicación que permitiese hacer todo este proceso de manera automatizada. Dicho protocolo, que pertenece a los llamados protocolos de infraestructura TCP/IP dentro del nivel de aplicación, se llama DHCP (Dynamic Host Configuration Protocol) o Protocolo para la Configuración Dinámica de Equipos, y define cómo conseguir una gestión centralizada y automatizada de las direcciones IP de los equipos de una red.**



El protocolo DHCP proporciona un mecanismo para que la asignación de direcciones IP a los equipos de una red pueda gestionarse de manera centralizada desde un equipo servidor. El resto de equipos le preguntan a dicho servidor, en el momento de arranque, cuál

es la dirección IP que deben utilizar y configuran su pila TCP/IP como corresponde. De esta manera, el administrador de la red no tiene que ir equipo por equipo configurando las direcciones IP de cada uno de ellos, sino que esta tarea puede realizarla en el propio servidor DHCP.

DHCP ofrece al administrador de la red un gran número de posibilidades a la hora de establecer la política a seguir para la asignación de las direcciones IP. Por ejemplo, entre otras cosas:

- Puede establecer que a cada ordenador se le asigne una dirección IP de manera aleatoria de entre las que haya disponibles en ese momento.
- Puede establecer que, a cada ordenador, identificado por la dirección MAC de su tarjeta de red, se le asigne siempre la misma dirección IP.
- Puede establecer rangos de direcciones asignables y no asignables.
- Puede establecer la duración que tiene la asignación de dicha dirección IP pasada la cual el ordenador deberá negociar su renovación.

El protocolo DHCP no sólo se utiliza para comunicarle a los equipos de la red cuál es la dirección IP que deben de tomar, también se utiliza para comunicarles el resto de información que necesitan para su correcto funcionamiento en la red, como: la máscara de subred que tienen que utilizar, cuál es la dirección del router que les da salida fuera de la subred y la dirección del servidor DNS que tienen que utilizar.

Puede plantearse varias dudas: ¿cómo es posible que el equipo “cliente DHCP” pueda comunicarse con el equipo “servidor DHCP” si aquél no tiene todavía dirección IP asignada? Y ¿cómo localiza el cliente al servidor?; es decir, ¿cómo conoce cuál es la IP del servidor?

- Para solucionar el primer problema, el protocolo establece que el cliente debe usar la dirección IP 0.0.0.0 (esta dirección la utiliza el equipo para referirse a sí mismo dentro de la red) como dirección origen mientras no tenga asignada una dirección IP propia.
- Para solucionar el segundo problema, el protocolo establece que el cliente debe usar la dirección IP 255.255.255.255 (esta dirección se refiere a todos los equipos de la subred) como dirección destino. Esto implica que el paquete IP llegará a todos los equipos de la red, aunque tan sólo lo procesará aquél equipo que esté configurado como “servidor DHCP”, pues será el único que tenga un proceso escuchando en el puerto correspondiente. Una vez que el servidor responde por primera vez al cliente, éste puede aprender la dirección IP del servidor y puede dirigirse a él de manera directa y no mediante broadcast durante el resto de la conversación.

El protocolo DHCP suele utilizarse mayormente en entornos de red de área local, aunque los operadores de acceso a Internet que utilizan la tecnología de cable también utilizan este protocolo para asignar direcciones IP a los ordenadores a los que dan servicio de conexión.

4.2. SERVICIO DNS

Cuando un usuario quiere que su aplicación establezca una comunicación con otra aplicación remota, debe de decirle la dirección IP de la máquina dónde se encuentra dicha aplicación remota. De hecho, si no se está utilizando un servicio estándar para el que haya establecido un puerto bien conocido, también tendría que indicarle el puerto en el que estará escuchando la aplicación remota con la que se quiere establecer la comunicación.

Es decir, si por ejemplo queremos que nuestro navegador Web se conecte a un servidor Web, debemos indicarle cuál es la dirección IP de dicho servidor. Imagina que tuvieras que conocer las direcciones IP de todos los servidores a los que te sueles conectar. ¿Cuántas serías capaz de recordar? Seguro que no muchas. De todas formas, cuando quieres establecer una conexión con un servidor en Internet, ¿nos referimos a él por su dirección IP? ¡No!, excepto en casos muy excepcionales, ¡hacemos referencia a un ordenador servidor haciendo uso de un nombre y no de una dirección IP! ¿Cómo puede ser esto posible? Pues **es posible gracias a un protocolo de aplicación de los llamados protocolos de infraestructura TCP/IP, cuyo nombre es DNS (Domain Name System) o Sistema de Nombres de Dominio, y cuya misión es la de hacer de traductor entre direcciones IP y nombres de dominio, proceso que recibe el nombre técnico de resolución de nombres.** Cada vez que hacemos referencia a un servidor de Internet por su nombre, internamente este nombre debe ser traducido a su dirección IP asociada, pues no debemos olvidar que el protocolo IP sigue utilizando las direcciones IP para localizar a los ordenadores en la interred. La existencia de nombres para identificar a los ordenadores obedece a una necesidad humana, no a una necesidad de los ordenadores.

4.2.1. ESTRUCTURA DEL SISTEMA DE NOMBRES DE DOMINIO

La tarea de resolución de nombres, es decir, de averiguar la dirección IP asociada al nombre de un ordenador, puede parecer simple en un principio, pero no perdamos de vista los siguientes tres grandes problemas a los que nos enfrentamos y que deben ser resueltos:

- La carga de trabajo es grandísima. Cada día hay billones de peticiones para que un nombre sea traducido a su dirección IP asociada.
- La tabla de traducción es enorme. Actualmente hay millones de direcciones IP en uso y hay muchísimos ordenadores que tienen un nombre asignado.
- Internet es una entidad dinámica que cambia cada día. Todos los días se crean nuevos nombres de dominio y otros desaparecen. Además, los nombres asignados a los ordenadores o incluso las direcciones asignadas a los mismos puede variar.

Por tanto, como puedes observar, no se trata de una tarea tan sencilla.

En los inicios de Internet, cuando la red no era muy grande y estaba formada por unos cuantos equipos, cada uno de los ordenadores conectados contaba con un fichero en el que había almacenada una tabla con la correspondencia entre direcciones IP y nombres, de tal manera

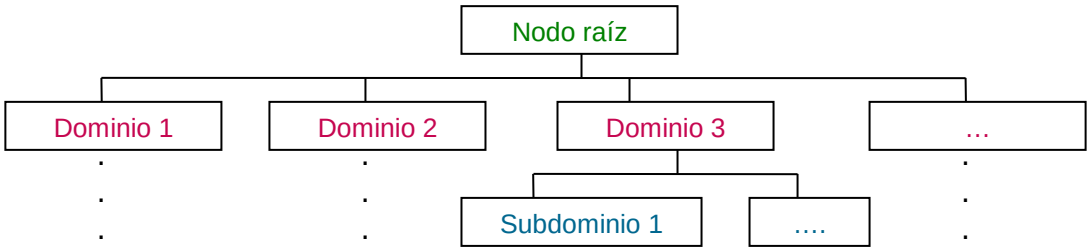
que consultando dicho fichero un ordenador podía hacer la traducción. Evidentemente, esto suponía que cada vez que hubiese el más mínimo cambio en el nombre o dirección de cualquier ordenador, había que actualizar uno a uno los ficheros de todos y cada uno de los ordenadores. Se pensó entonces en disponer de un ordenador central en el que estuviese almacenado dicho fichero de traducción de nombres y que el resto de los ordenadores se conectase a él para bajarse el fichero cada cierto tiempo, de tal manera que éstos tuviesen actualizada siempre la información. Con el crecimiento de Internet esta idea también se volvió inviable, pues la conexión simultánea de millones de ordenadores al mismo ordenador central para la descarga del fichero produciría una caída del servicio.

Se pensó entonces en la creación de un sistema que:

- **Fuese un sistema distribuido** - La información de traducción no debía estar centralizada en un único ordenador, para evitar que el acceso masivo de usuarios solicitando dicha información lo bloquease. Lo que debía hacerse era distribuir la información de traducción entre muchos ordenadores que pudiesen repartirse la carga del trabajo de resolución de nombres. Además, dado el enorme tamaño de la tabla de traducción, la resolución de nombres se convertía en una tarea lenta. Para acelerar la búsqueda en la tabla y, por tanto, la resolución de nombres, lo que debía hacerse era partir la tabla de traducción de nombres en varias partes y distribuir éstas entre distintos ordenadores, de tal manera que cada uno de ellos manejase sólo una parte de la tabla, que sería muchísimo más pequeña que la original y, consecuentemente, más rápido el proceso de búsqueda en la misma.
- **Fuese un sistema jerárquico** - No debía haber un único organismo que controlase y gestionase la asignación de los nombres a los ordenadores, sino que se necesitaba una estructura más flexible que pudiese dar respuesta y adaptarse al dinamismo que caracteriza a Internet. Lo que debía hacerse era crear una organización en la que se delegasen las competencias en distintas autoridades que fuesen capaces de autogestionarse, aunque estuviesen supervisadas por una autoridad superior. Se pensó entonces que lo mejor era reproducir la estructura jerárquica en forma de árbol en la que se organiza la cadena de mando de una empresa, la cual se divide en departamentos que se autogestionan, si bien cada uno de ellos tenga siempre que rendir cuentas al eslabón superior en la jerarquía. Además, se decidió que cada una de estas autoridades de segundo nivel podrían a su vez volver a delegar en autoridades de nivel inferior a las cuales se encargaría de supervisar, y así sucesivamente.

Este sistema descrito lo conocemos con el nombre de Sistema de Nombres de Dominio o DNS, el cual no es más que una **base de datos distribuida y estructurada jerárquicamente en forma de árbol**.

Este sistema de nombres de dominio consiste en una base de datos distribuida y estructurada jerárquicamente en forma de árbol:

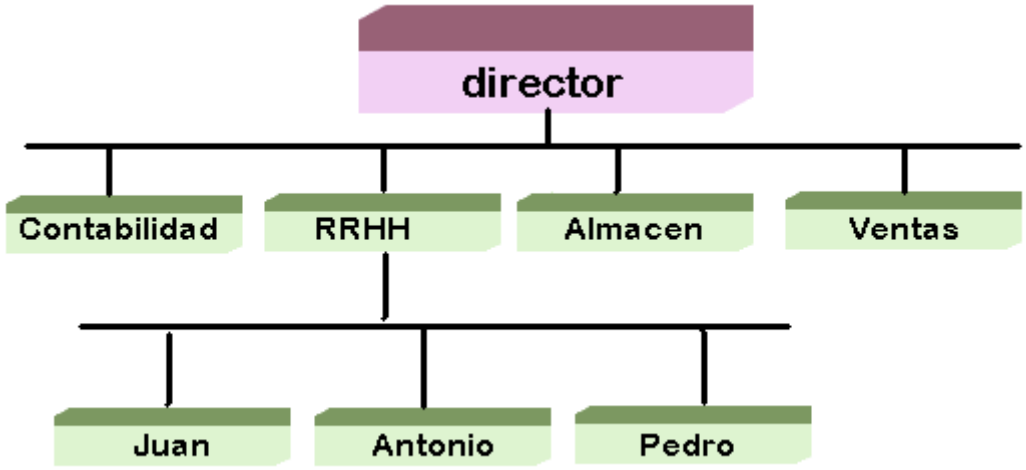


- Nodo raíz – Es el nodo principal de la estructura.
- Dominios ≅ **dominios de primer nivel –** Son los hijos del nodo raíz, cada uno de ellos tiene que encargarse de conocer la traducción entre IP y nombre de todos los ordenadores que estén bajo su responsabilidad; es decir, bajo su "dominio".
- Subdominios – Son la división de los dominios en unidades más pequeñas.

EJEMPLO

Imagina una empresa gigantesca, con millones de trabajadores, en la cual cada trabajador tiene un DNI y un nombre. De cara a la empresa y a la Administración del Estado, lo que identifica a cada trabajador es su DNI; sin embargo, evidentemente, las personas no conocen ni se dirigen a sus compañeros por su DNI, sino por su nombre. Por lo tanto, para realizar cualquier gestión en la empresa, por ejemplo, hacer las nóminas de los trabajadores, tiene que implementarse algún mecanismo para, dado el nombre de un trabajador, poder averiguar cuál es su DNI. Imagina además que la empresa es muy dinámica y que cada día se incorporan nuevos trabajadores y otros tantos la abandonan. Como puedes observar, nos enfrentamos a un problema semejante al descrito para la resolución de nombres en Internet, y vamos a resolverlo creando un sistema de traducción que siga las pautas que establecimos para el sistema DNS: un sistema distribuido y organizado jerárquicamente en forma de árbol. Para ello vamos crear un sistema que utilice la estructura en árbol de los departamentos de la propia empresa. En dicha estructura organizativa en árbol hay un nodo raíz, o punto principal de la estructura, que estará formado por el equipo directivo o junta de administración de la empresa; es decir, los jefes. A partir de este nodo raíz surgen una serie de departamentos de primer nivel o departamentos principales de la empresa. Dichos departamentos tienen capacidad de autogestión, aunque dependan directamente del nodo raíz, ante el cual tienen que rendir cuentas. Así, y poniendo en práctica la filosofía de distribución de la información y delegación de responsabilidades de gestión, cada departamento será el encargado de gestionar la información asociada a los trabajadores que trabajan en él y de conocer la traducción entre DNI y nombre de los mismos. Además, cada departamento puede a su vez dividirse en departamentos de nivel inferior en los cuales delegar y los cuales se compromete a supervisar. Con este sistema implantado, si una persona de la empresa necesita conocer el DNI asociado a un trabajador que trabaja en su mismo departamento, le tendrá que preguntar al responsable

de personal del mismo, pues es el que gestiona la información interna del departamento. Sin embargo, si la información que se necesita es de un trabajador externo al departamento, entonces le tendrá que preguntar al responsable de personal del departamento al que pertenece el trabajador del que se quiere obtener la información.



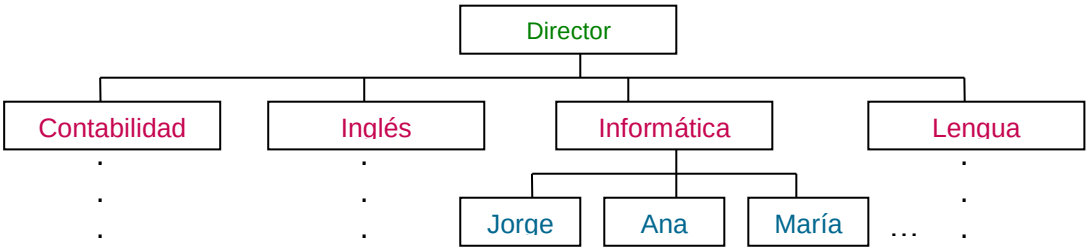
Pues bien, el sistema DNS es muy semejante al sistema anteriormente descrito. Así:

- Existe un **nodo raíz** de la estructura
- Del nodo raíz surgen una serie de hijos, llamados **dominios de primer nivel o simplemente dominios**, donde cada uno de ellos tiene capacidad de autogestión, al igual que lo tenían los departamentos del ejemplo, y cada uno de ellos tiene que encargarse de conocer la traducción entre IP y nombre de todos los ordenadores que estén bajo su responsabilidad; es decir, bajo su "dominio".
- Cada dominio tiene potestad para decidir dividirse a su vez en unidades más pequeñas con capacidad de autogestión, llamadas **subdominios**.

EJEMPLO

Imagina un instituto en el cual cada profesor tiene su DNI (el identificador de cada profesor) y su nombre. Podemos crear un sistema que utilice la estructura en árbol de los departamentos del instituto. Dicha estructura está formada por:

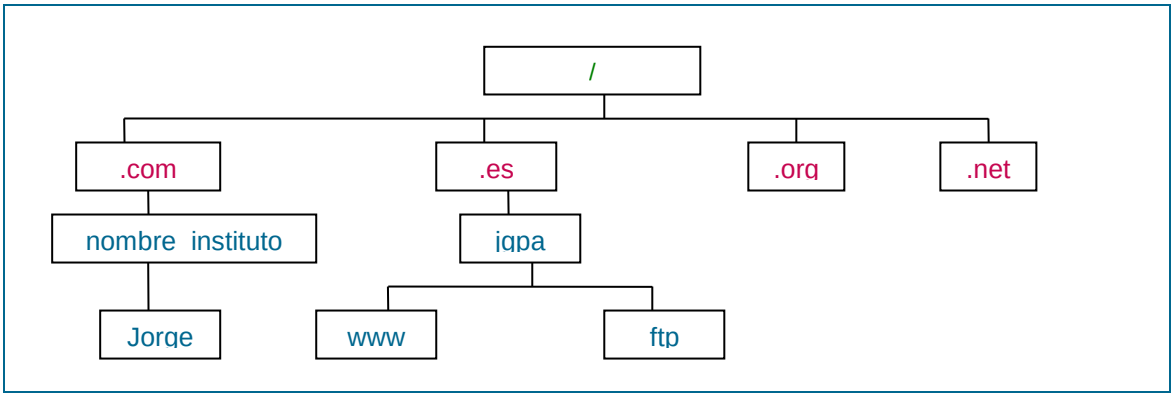
- Nodo raíz – En este ejemplo es el director.
- Dominios – Incluye los departamentos principales o de primer nivel del instituto. Estos departamentos dependen del nodo raíz y deben conocer la traducción entre DNI y nombre de los profesores de su departamento, también se encargarán de gestionar la información
- Subdominios – Serían departamentos de nivel inferior si los hubiera. En este caso los subdominios serán los profesores de cada departamento.



EJEMPLO

El siguiente ejemplo muestra una estructura de direcciones web:

- Nodo raíz – En este ejemplo es el directorio raíz /.
- Dominios – Incluye dominios asociados a un tipo de actividad concreto: com, es, org, net
- Subdominios – Se refiere a: nombre_instituto, jgpa
- Subdominios – Se refiere a: jorge, www, ftp



Hay centenares de dominios de primer nivel, cada uno de los cuales está asociado, generalmente, a un tipo de actividad concreto, si bien es cierto que esto ha quedado ya un poco desvirtuado.

Esta es una lista, bastante completa, de nombres de dominio de primer nivel (Top Level Domain names), empezando con los "genéricos":

.**com** Entidad u organización comercial

.org Organización no-lucrativa (técnicamente)

.**net** Redes u organizaciones dedicadas a la red

.int Organización de tratado internacional (p.e. http://www.nato.int/)

.edu Institución educacional

.gov Cuerpo, departamento o agencia gubernamental (p.e. http://www.fbi.gov/)

.mil Sitio militar

Se ha propuesto la inclusión de siete nuevos dominios de primer nivel, pero de momento no son más que recomendaciones:

.firm para negocios o empresas

.store para tiendas o empresas que ofrecen bienes para comprar

.web para entidades relacionadas con la w.w.w.

.arts para entidades de actividades culturales

.rec para entidades de actividades recreativas

.info para entidades de servicios de información

.nom para individuos que quieren un nombre o pseudónimo personal

El resto de los dominios corresponden a los códigos de países según la norma ISO 3166. Algunos, como el Reino Unido, incluyen un dominio funcional de segundo nivel, p.e. "univ.ac.uk" será una institución académica, mientras "empresa.co.uk" sería una compañía. Se ha recomendado el uso de .tm como dominio de segundo nivel para distinguir marcas patentadas (trademarks), junto con cualquier dominio de primer nivel, pero todavía no se utiliza.

Los códigos de países están por orden alfabético.

AD Andorra
AE Emiratos Arabes Unidos
AF Afghanistán
AG Antigua y Barbuda
AI Anguilla
AL Albania
AM Armenia
AN Antillas Holandesas
AO Angola
AQ Antartica
AR Argentina
AS Samoa Oriental
AT Austria
AU Australia
AW Aruba
AZ Azerbeiján
BA Bosnia-Herzegovina
BB Barbados
BD Bangladesh
BE Bélgica
BF Burkina Fasso (Alta Volta)
BG Bulgaria
BH Bahrein
BI Burundi
BJ Benin
BM Bermuda
BN Brunei
BO Bolivia
BR Brazil
BS Bahamas
BT Bután
BV Bouvet Island
BW Botswana
BY Bielorrusia
BZ Belice
CA Canadá
CC Cocos (Islas)
CF República Centroafricana
CG Congo
CH Suiza
CI Costa de Marfíl
CK Islas Cook
CL Chile
CM Camerún
CN China
CO Colombia
CR Costa Rica
CU Cuba
CV Cabo Verde
CX Christmas (Isla)
CY Chipre
GP Guadaloupe
GQ Guinea Equatorial
GR Grecia
GT Guatemala
GU Guam
GW Guinea-Bissau
GY Guyana
HK Hong Kong
HM Islas Heard y McDonald
HN Honduras
HR Croacia
HT Haití
HU Hungría
ID Indonesia
IE Irlanda
IL Israel
IN India
IO Teritorias Británicas Oceano Indico
IQ Iraq
IR Iran
IS Islandia
IT Italia
JM Jamaica
JO Jordánia
JP Japón
KE Kenia
KG Kyrgyzstan
KH Cambodia
KI Kiribati
KM Comoros
KN Saint Kitts y Nevis
KP Corea
KR Corea (República de)
KW Kuwait
KY Islas Cayman
KZ Kazakhstan
LA Lao
LB Lebanon
LC Santa Lucía
LI Liechtenstein
LK Sri Lanka
LR Liberia
LS Lesotho
LT Lituania
LU Luxemburgo
LV Latvia
LY Libyan Arab Jamahiriya
MA Morocco
MC Mónaco
MD Moldova
MG Madagascar
MH Islas Marshall
MK Macedonia
NU Niue
NZ Nueva Zelanda
OM Omán
PA Panamá
PE Peru
PF Polinesia Francesa
PG Papua Nueva Guinea
PH Filipinas
PK Pakistán
PL Polonia
PM Saint Pierre y Miquelón
PN Pitcairn
PR Puerto Rico
PT Portugal
PW Palau
PY Paraguay
QA Qatar
RE Reunión
RO Romania
RU Federación Rusa
RW Ruanda
SA Arabia Saudí
SB Islas Solomón
SC Seychelles
SD Sudán
SE Suecia
SG Singapur
SH Santa Helena
SI Eslovenia
SJ Islas Svalbard y Jan Mayen
SK Eslovaquia
SL Sierra Leona
SM San Marino
SN Senegal
SO Somalia
SR Surinam
ST Sao Tome y Principe
SU Antigua Unión Soviética
SV El Salvador
SY Siria
SZ Swazilandia
TC Islas Turks y Caicos
TD Chad
TF Territotias Franceses del Sur
TG Togo
TH Tailandia
TJ Tajikistan
TK Tokelau
TM Turkmenistan
TN Tunísia
TO Tonga
TP Timor Oriental

CZ República Checa
DE Alemania
DJ Djibuti
DK Dinamarca
DM Dominica
DO Repú:blica Dominicana
DZ Argelia
EC Ecuador
EE Estonia
EG Egipto
EH Sáhara Occidental
ES España
ET Etiopía
FI Finlandia
FJ Fidji
FK Islas Malvinas
FM Micronesia
FO Islas Faroe
FR Francia
GA Gabón
GD Grenada
GE Georgia
GF Guiana Francesa
GH Ghana
GI Gibraltar
GL Groenlandia
GM Gambia
GN Guinea
ML Mali
MM Myanmar
MN Mongolia
MO Macau
MP Northern Mariana Islands
MQ Martinica
MR Mauritania
MS Montserrat
MT Malta
MU Mauricio
MV Maldivas
MW Malawi
MX Méjico
MY Malasia
MZ Mozambique
NA Namibia
NC Nueva Caledonia
NE Niger
NF Norfolk Island
NG Nigeria
NI Nicaragua
NL Paises Bajos
NO Noruega
NP Nepal
NR Nauru
NT Zona Neutral (entre SA y IQ)
TR Turquía
TT Trinidad y Tobago
TV Tuvalu
TW Taiwan
TZ Tanzania
UA Ukrania
UG Uganda
UK Reino Unido
UM EE.UU. Islas Menores
US Estados Unidos
UY Uruguay
UZ Uzbekistan
VA Vaticano
VC San Vicent y los Grenadines
VE Venezuela
VG Islas Vígenes (Británicos)
VI Islas Vírgenes (EE.UU.)
VN Vietnam
VU Vanuatu
WF Islas Wallis y Futuna
WS Samoa
YE Yemen
YU Yugoslavia
ZA Sudafrica
ZM Zambia
ZR Zaire
ZW Zimbabwe

La **organización supranacional ICANN** coordina la administración de los elementos técnicos del DNS para garantizar la resolución unívoca de los nombres, para que los usuarios puedan encontrar todas las direcciones sin ser repetidas. En la actualidad, la ICANN está formalmente organizada como una corporación sin fines de lucro y de utilidad pública.

4.2.2. EL NOMBRE DE DOMINIO

Si observamos detenidamente el nombre de un ordenador en el sistema DNS, nos daremos cuenta de que éste no es un nombre plano, sino que refleja esta estructura jerárquica que estamos describiendo. Es decir, el nombre no sólo identifica a un ordenador, sino que además aporta información acerca de la situación del mismo en la jerarquía: el propio nombre DNS del ordenador nos dice el subdominio al que pertenece dentro de la jerarquía de dominios y subdominios.

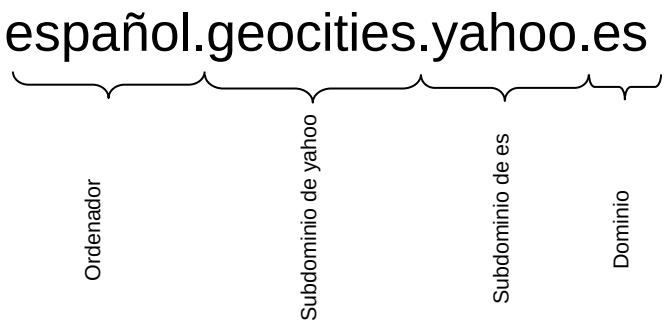
EJEMPLO

Sea un ordenador cuyo nombre DNS es “español.geocities.yahoo.es”, dicho nombre podemos dividirlo en cuatro partes, cada una de las cuales viene separada de las otras por un punto. Dichas partes, analizando el nombre de derecha a izquierda son:

- El **nombre del dominio de primer nivel**, o simplemente **dominio**, al que pertenece el ordenador. En este caso al dominio “.es”; es decir, es un ordenador que pertenece al dominio administrado por España.

- El nombre del **subdominio, dentro del dominio ".es"**, al que pertenece el ordenador. En este caso al subdominio "yahoo".
- El nombre del **subdominio, dentro del subdominio "yahoo"**, al que pertenece el ordenador. En este caso al suddominio "geocities".
- El **nombre del ordenador** dentro del subdominio "geocities". En este caso el ordenador tiene el nombre de "español".

Por lo tanto, al indicar que queremos establecer una comunicación con el ordenador "español.geocities.yahoo.es", estamos indicando que queremos contactar con el ordenador llamado "español", que pertenece al subdominio "geocities", que a su vez forma parte del subdominio "yahoo", dentro del dominio ".es".



Como podemos observar, cada organización o entidad propietaria de un dominio, o subdominio, tiene potestad para administrarlo como desee y para poner a los ordenadores que gobierna los nombres que desee. La única condición que se impone es que no otorgue dos veces el mismo nombre. Así, por ejemplo:

- No puede haber dos dominios de primer nivel con el mismo nombre. No puede haber dos dominios ".com"
- **Un dominio de primer nivel no puede crear dos subdominios con el mismo nombre**. Es decir, por ejemplo, en España no puede haber dos subdominios registrados en el dominio ".es" que tengan el mismo nombre, no puede haber dos "jgpa.es".
- Igualmente, un subdominio dividido a su vez en subdominios, no puede crear dos subdominios de nivel inferior con el mismo nombre. Es decir, por ejemplo, la Junta General del Principado de Asturias no puede crear dos subdominios con el mismo nombre dentro de su subdominio "jgpa.es".
- Por último, un subdominio no dividido en subdominios, no puede asignar el mismo nombre a dos ordenadores distintos.

Sin embargo, sí son posibles las siguientes situaciones:

- Que dos ordenadores pertenecientes a subdominios distintos tengan el mismo nombre. Por ejemplo, dos ordenadores que se llaman “WWW”; sin embargo, su nombre completo DNS no es el mismo: “www. jgpa.es” y “www.valliniello.com”.
- Que dos subdominios tengan el mismo nombre, siempre y cuando no tengan el mismo subdominio padre. Es decir, por ejemplo, “www.elmundo.es” y “www.elmundo.com”, donde hay dos subdominios con el mismo nombre, “elmundo”, pero que no hay ningún conflicto entre ellos porque uno depende del dominio de primer nivel “es” y el otro del dominio de primer nivel “com”. Por tanto, su nombre completo DNS no es el mismo.

4.2.3. EL PROCESO DE RESOLUCIÓN DE NOMBRES DE DOMINIO

Ya sabemos cómo es la arquitectura de lo que conocemos como Sistema de Nombres de Dominio o DNS, pero ¿qué sucede cuando se solicita la resolución de un nombre? ¿A quién se le solicita? ¿Qué proceso se desencadena para que a partir de un nombre DNS se pueda obtener la dirección IP del ordenador al que pertenece dicho nombre? El elemento clave para dar respuesta a estas preguntas es el conocido con el nombre de servidor de nombres o servidor DNS.

Todo ordenador conectado a Internet debe conocer la IP de al menos un **servidor DNS** al que pueda hacer peticiones de resolución de nombres. Un servidor de nombres es un ordenador, o más correctamente dicho, una aplicación ejecutándose en un ordenador, que tiene asignadas las siguientes dos tareas:

- Aceptar y atender peticiones de usuarios que le solicitan que les convierta un nombre de dominio en su dirección IP asociada.
- Aceptar y atender peticiones de otros servidores de nombres que le solicitan que les convierta un nombre de dominio en su dirección IP asociada.

Cuando un servidor de nombres recibe una petición puede hacer una de las siguientes cuatro cosas:

- Puede responder directamente a la petición si es que ya conoce cuál es la dirección IP asociada al nombre de dominio solicitado.
- Puede contactar con otro servidor de nombres para tratar de averiguar la dirección IP asociada al nombre de dominio solicitado. De hecho, puede tener que contactar con varios otros servidores DNS.
- Puede responder algo así como: “No conozco la dirección IP asociada al nombre de dominio que me pides, pero te voy a facilitar la dirección IP de otro servidor DNS que sabe más de lo que yo sé”.
- Puede responder con un mensaje de error porque el nombre de dominio que debe resolver no es válido o no existe.

Imagina que una aplicación que estás ejecutando en tu ordenador necesita comunicarse con otro ordenador cuyo nombre es “www. jgpa.es”. Entonces:

- Dicha aplicación contactará con el servidor DNS establecido en la configuración de red del ordenador en el que se está ejecutando, en lo sucesivo llamado servidor DNS local, y le dirá algo así como: “Necesito que me digas cuál es la dirección IP asociada al nombre de dominio www.jgpa.es”.
- Puede ser que dicho servidor DNS conozca la respuesta a la pregunta planteada, por ejemplo, si ya la contestó recientemente, en cuyo caso la tendrá almacenada en su caché. En ese caso, podrá contestar a la pregunta él mismo y de manera inmediata.
- Supongamos, sin embargo, que el servidor DNS local no conoce la respuesta. Entonces, dicho servidor contactará con uno de los servidores DNS raíz, donde un servidor DNS raíz es un servidor de nombres que conoce las direcciones de todos los servidores DNS encargados de gestionar los dominios de primer nivel, y le preguntará por la resolución del nombre. Si éste tampoco sabe la respuesta, pues no la tiene en su caché, le contestará al servidor DNS local proporcionándole la dirección IP del servidor de nombres encargado de gestionar el dominio de primer nivel al que pertenece el nombre a resolver. En nuestro ejemplo, éste servidor raíz contestaría algo así como: “No conozco la IP asociada al nombre www. jgpa.es, pero te facilito la dirección IP del servidor de nombres que gestiona el dominio .es”. Evidentemente, los servidores DNS raíz son vitales en este proceso, por lo que hay muchos de ellos repartidos por todo el planeta. Además, cada servidor DNS tiene una lista de todos los servidores raíz conocidos. En caso de necesidad, contactará con el primero de dicha lista y si no puede establecer contacto por alguna razón, entonces irá sucesivamente intentándolo con los sucesivos servidores DNS raíz listados.
- Una vez que el servidor de nombres local recibe la respuesta del servidor DNS raíz, lanzará la pregunta de resolución de nombres al servidor de primer nivel correspondiente. En nuestro caso al servidor DNS que gestiona el dominio .es.
- Nuevamente, si dicho servidor DNS conoce la respuesta, la contestará él mismo al servidor de nombres local. En caso contrario, le responderá con la dirección IP del servidor DNS encargado de gestionar el subdominio jgpa.es, la cual debe conocer, ya que todo servidor de nombres tiene la obligación de conocer las direcciones de todos aquellos servidores DNS en los que ha delegado la gestión de sus subdominios.
- El servidor de nombres local contactará entonces con dicho servidor DNS, el cual obligatoriamente conoce la dirección IP asociada al nombre www.jgpa.es, pues es un nombre que se encuentra directamente bajo su dominio. Por tanto, éste servidor sí que será capaz de contestar a la pregunta de resolución de nombres.

- Cuando el servidor de nombres local recibe la respuesta, ya provenga ésta desde este último servidor DNS que rige el dominio jgpa.es, o bien desde cualquier otro anterior que conociese la respuesta al tenerla almacenada en su caché, entonces ya está en disposición de contestarle a la aplicación de tu ordenador que inició el proceso.

5. SERVICIOS EN INTERNET

Para conseguir que Internet sea realmente útil es necesario conocer los servicios que pone a nuestra disposición y además saber utilizarlos de forma correcta. Si no los conocemos, no podremos usarlos y si no los usamos correctamente, podemos llegar a complicar las cosas de forma que no compense la utilidad que proporcionan con el trabajo que conllevan.

Habiendo terminado de ver algunos de los protocolos de apoyo o de infraestructura TCP/IP usados en la capa de aplicación, por fin llegamos a las aplicaciones concretas, aquellas con las que interactúan los usuarios. A la pregunta: “¿qué vas a hacer ahora?”, poca gente contestará: “voy a buscar algunos nombres con el DNS”. La gente dice que va a leer su correo electrónico, a navegar por la Web, a transferir un archivo, o a conectarse a un ordenador remoto en el que tiene que trabajar. Todas estas aplicaciones o servicios de Internet son los que utilizan directamente los usuarios para alcanzar sus fines.

Las posibilidades para la comunicación, acceso a información y ocio que nos ofrece Internet son ilimitadas. En la Red, la comunicación siempre se produce entre dos aplicaciones que se encuentran en ordenadores distintos, las cuales, según el propósito que persigan con dicha comunicación, usarán un protocolo u otro de entre los llamados protocolos de nivel de aplicación en el modelo TCP/IP. La mayoría de estos protocolos de aplicación, aunque no todos, siguen lo que se conoce como modelo cliente-servidor.

De igual manera que en la vida real hay ciertas entidades que ofrecen servicios, por ejemplo, servicio de peluquería, servicio de venta de pan, servicio de lavado de coches, etc., en el mundo de Internet hay aplicaciones ejecutándose en ordenadores, las cuales desempeñan el papel de servidores al ofrecer ciertos servicios a quien pudiera solicitarlos. Análogamente, si en la vida real hay otras entidades que requieren dichos servicios ofertados y hacen uso de ellos, en el mundo de Internet también hay aplicaciones ejecutándose en ciertos ordenadores y desempeñando el papel de clientes, al solicitar alguno de los servicios disponibles.

EJEMPLO

En el modelo de comunicación cliente-servidor, de las dos aplicaciones involucradas en la comunicación hay una que es la que ofrece el servicio, y recibe el nombre de servidor, y hay otra es la que solicita el servicio, y recibe el nombre de cliente. El cliente es una aplicación que usando las reglas establecidas en el protocolo de aplicación que esté utilizando, ejecuta peticiones que son enviadas a través de la red a la aplicación servidora. Por su parte, el servidor o aplicación servidora permanece a la escucha en un puerto del ordenador a través del cual le irán llegando dichas peticiones. Entonces, la aplicación servidora realizará las tareas necesarias para servirlas y responderá al cliente con los resultados. Podemos observar que en este modelo el cliente es el que lleva la iniciativa en cada solicitud, mientras que el servidor se limita a seguir las órdenes cursadas por el cliente.

Los servicios que se ofrecen en Internet son muy variados, pero los cuatro más importantes son los siguientes:

- **El servicio Web** - Proporciona a los usuarios la capacidad de consultar información alojada en otros ordenadores en formato de páginas electrónicas o páginas Web.
- **El servicio de correo electrónico** - Proporciona capacidad a los usuarios de la red para redactar, enviar y recibir mensajes.
- **El servicio de transferencia de archivos** - Proporciona a los usuarios la capacidad para alojar archivos en un ordenador remoto y descargarlos posteriormente.

- **El servicio de inicio remoto de sesión** - Proporciona a los usuarios la capacidad de que puedan iniciar una sesión en cualquier otro ordenador en el que tengan una cuenta.

5.1. SERVICIO WEB

A finales de los años 80 Internet había alcanzado ya un tamaño considerable y el volumen de información disponible en los distintos ordenadores conectados habían convertido esta red en el mayor almacén de datos de la historia. Sin embargo, su crecimiento, un tanto caótico y desordenado, había hecho que la búsqueda y el acceso a dicha información fuese una tarea muy difícil: cada uno almacenaba sus datos utilizando un formato distinto y, por tanto, distintos eran los protocolos utilizados para acceder a ellos. Internet era una red de uso complejo sólo apta para investigadores y técnicos. Su interfaz era textual (de texto) y los comandos para manejarla, complejos. Se hicieron necesarias nuevas formas para indicar la posición de un documento a recuperar y para navegar a través de la red; es decir, se vio entonces la necesidad de llegar a un acuerdo para almacenar la información en un formato común, que permitiese un acceso homogéneo haciendo uso de un mismo protocolo. Como respuesta a estas necesidades, a principios de los 90 nace en el seno del **CERN** (Conseil Européen pour la Recherche Nucléaire) o Consejo Europeo para la Investigación Nuclear, y de manos de Tim Berners Lee, la World Wide Web, la telaraña mundial o simplemente la Web: un foro de intercambio de información y un mercado en crecimiento accesible a cualquier usuario, independientemente de su grado de conocimiento teórico. Este nuevo servicio de Internet recibió el nombre de servicio Web; su misión: proporcionar a los usuarios la capacidad de consultar información alojada en otros ordenadores en formato de páginas electrónicas o páginas Web. Veamos qué se oculta detrás de este servicio que ha sido, sin duda alguna, el máximo responsable del increíble auge que ha experimentado Internet desde 1993.

Actualmente la Web es administrada por el **World Wide Web Consortium** o **consorcio de la Web**, cuya misión es la de promover el crecimiento de la Web por medio del desarrollo de especificaciones de referencia que luego son puestas a disposición de toda la comunidad sin costo alguno.

5.1.1. ARQUITECTURA DEL SERVICIO WEB

El servicio Web sigue el modelo cliente-servidor y, como en cualquier otro servicio que siga dicha filosofía, en el proceso de comunicación hay una aplicación que desempeña el papel de servidor y otra que desempeña el papel de cliente:

- **El servidor** - En el servicio Web, la aplicación que desempeña el papel de servidor recibe el nombre de Servidor Web, y su misión es la de poner a disposición de los clientes una serie de recursos.

Dentro del mundo de los servidores Web destacamos los dos más populares: dentro de lo que se conoce como Software Propietario, "**Internet Information Server**", y dentro de lo que se conoce como Software Libre, "**Apache Web Server**".

- **El cliente** - Por su parte, la aplicación que desempeña el papel de cliente en una comunicación Web, recibe el nombre de **Navegador Web**, y su misión es la de solicitar al servidor la entrega de alguno de los recursos que ofrece.

  Desde la aparición en 1993 del primer navegador, llamado **Mosaic**, son muchos los disponibles en el mercado, siendo dos los más populares: dentro de lo que se conoce como Software Propietario, el Internet Explorer de Microsoft, y dentro de lo que se conoce como Software Libre, el Mozilla Firefox.

Como puedes imaginar, **la comunicación entre un navegador y un servidor Web se encuentra perfectamente reglada en un protocolo de nivel de aplicación**. Las reglas que rigen una comunicación Web entre un navegador y un servidor Web, vienen recogidas en un **protocolo** llamado **HTTP** (HyperText Transport Protocol) o Protocolo para la Transferencia de Hipertexto.

El propio nombre del protocolo, HTTP, hace referencia a qué es lo que intercambian cliente y servidor durante su comunicación: **Hipertexto**. Se plantea entonces la siguiente pregunta clave, ¿qué es el hipertexto? Podemos definir **hipertexto como un documento digital que se puede leer de manera no secuencial. Básicamente, un documento de hipertexto es un fichero formado únicamente por dos tipos de elementos:**

- **Texto**
- **Referencias a otros documentos de hipertexto** - Estas referencias son zonas especiales del documento las cuales, al pinchar sobre ellas con el ratón, producen la solicitud a cualquier otro servidor Web de otro documento de hipertexto. Estas referencias, llamadas **hiperenlaces**, **enlaces, vínculos o hipervínculos**, son la piedra angular de la World Wide Web, siendo incluso el origen del propio nombre del servicio, "la telaraña" (the web), el cual hace referencia a esa maraña de referencias que se forman en la Web entre distintos documentos de hipertexto. ¿De dónde crees

que procede el nombre de navegar por la Web? Pues precisamente de ese recorrido no secuencial de un documento a otro que se produce conforme se van visitando los enlaces.

HIPERTEXTO = TEXTO + HIPERENLACES

Seguro que ahora mismo te estás haciendo la siguiente pregunta: si un documento de hipertexto está formado únicamente por texto e hiperenlaces, ¿qué sucede con las fotos y resto de elementos que componen una página Web? Evidentemente, estos elementos no son texto; sin embargo, a la hora de ser transmitidos desde el servidor al cliente, utilizando unos mecanismos especiales, son codificados en forma de texto, para ser reconstruidos a su forma original en el destino. Es por eso que, a todos los efectos, de cara a HTTP son considerados como texto.

El diálogo que se produce entre navegador y servidor Web; es decir, el protocolo HTTP, es muy sencillo. Básicamente consiste en lo siguiente:

- El navegador solicita un recurso a un servidor Web.
- El servidor Web entrega dicho recurso al navegador, el cual lo visualiza.

Un recurso será generalmente una página Web, pero puede ser perfectamente una foto, un documento PDF, un documento de un procesador de textos o, en general, un fichero de cualquier otro tipo. Por tanto, de forma genérica, se llama recurso a cualquier fichero alojado en un servidor y accesible por los clientes haciendo uso del protocolo adecuado, en nuestro caso, el protocolo HTTP.

5.1.2. DIRECCIÓN WEB O URL

Por tanto, tal y como acabamos de describir en el apartado anterior, la función de un navegador Web es la de solicitar recursos; pero para poder hacerlo, tiene que haber una manera de especificar exactamente qué recurso se quiere, tiene que idearse una forma de identificar un recurso de manera unívoca en toda la Red. Para ello se utiliza lo que se conoce con el nombre de **URL** (Uniform Resource Locator) o **Localizador Uniforme de Recursos**, que no es más que una cadena de caracteres gracias a la cual se puede localizar cada uno de los recursos de información disponibles en la Web. Para localizar un recurso en la Red es necesario:

- Localizar al servidor Web en el que se encuentra el recurso buscado.
- Localizar el recurso dentro del servidor Web en el que se encuentra alojado.

Consecuentemente, una URL está formada por las siguientes partes perfectamente diferenciadas:

- Especificación del **protocolo o servicio** mediante el cual se pretende recuperar el recurso del servidor, seguido de “://”
- **Localización en Internet de la aplicación servidor Web en la que se encuentra el recurso buscado**. Debemos recordar que para localizar una aplicación en el modelo

de comunicación TCP/IP, deberemos proporcionar tanto la dirección IP del ordenador en el que se está ejecutando dicha aplicación, o en su defecto su nombre DNS, más el puerto en el que se encuentra escuchando dicha aplicación, ambos separados por ":". **El puerto bien conocido para los servidores Web es el puerto 80**, por lo que, si el servidor se encuentra escuchando en ese puerto, no será necesario especificar el puerto en la URL, pues se supondrá dicho puerto por defecto.

- **Localización en el servidor Web del recurso**. Para localizar el recurso dentro del servidor Web, deberá especificarse la ruta hasta el mismo.

EJEMPLO

URLs con sus recursos solicitados:

URL	Recurso Solicitado
http://www.mec.es/	index.html (página web) Al no decir nada toma por defecto el recurso index.html
http://www.mec.es/index.html	index.html (página web)
http://www.mec.es:80/index.html	index.html (página web)
http://www.mec.es:8080/	Da error porque no hay ningún servidor Web escuchando en ese puerto
http://www.mec.es/mecd/novedades/index.html	index.html (página web)
http://www.jgpa.es/SP/JDA/CDA/Imagenes/JDA-marca_junta.gif	JDA-marca_junta.gif (imagen)

5.1.3. EL RECURSO POR EXCELENCIA: LA PÁGINA WEB

Anteriormente definimos recurso como cualquier fichero que se encuentra alojado en un servidor y accesible por los clientes haciendo uso del protocolo adecuado, en nuestro caso, el protocolo HTTP. Sin embargo, aunque cualquier fichero es considerado un recurso, es cierto que la mayoría de los recursos que se solicitan en la Web son unos llamados páginas Web. ¿Y qué es exactamente una página Web? **Una página Web es un fichero de texto, generalmente con extensión .htm o .html, que se encuentra escrito en un lenguaje**

llamado HTML (HyperText Markup Language) o **Lenguaje de Marcado de Hipertexto**. Dicho lenguaje es un lenguaje de etiquetas o marcas que está diseñado para estructurar textos y presentarlos en forma de hipertexto, y el cual se engloba dentro de los llamados lenguajes de visualización, pues su única misión la de indicarle al navegador cómo debe presentar los contenidos que componen la página. Además, una página Web, aparte de hiperenlaces a otras páginas, puede incluir referencias a otros recursos como fotos, animaciones, etc. que se mostrarán incluidos en la propia página en el navegador, aunque sean recursos distintos que se solicitan de manera independiente a sus servidores correspondientes.

5.1.4. SEGURIDAD EN LA WEB

¿Has utilizado alguna vez el servicio de banca electrónica de algún banco? Si lo has hecho, te habrás dado cuenta de que la URL que introduces en la barra de direcciones del navegador no comienza por http, sino por https. ¿Qué es HTTPS? **HTTPS es un protocolo que permite la transmisión segura de información entre el navegador y el servidor Web mediante el uso de mecanismos de cifrado y certificados de autenticación, los cuales aseguran respectivamente**:

- Que si la información es interceptada por el camino no podrá ser leída, pues se asegura que ésta sólo podrá ser leída por el destinatario de la misma.
- Que los actores implicados en la comunicación son quienes dicen ser. Es decir, en el ejemplo del banco, que la Web pertenece realmente a la entidad bancaria en cuestión y que el usuario que está al otro lado del navegador es realmente el cliente del banco que dice ser.

Podríamos decir que HTTPS no es más que una variante segura de HTTP. Por razones más que evidentes, éste y no HTTP es el protocolo que utilizan los servidores Web de los bancos, pues la información que de allí se obtiene es confidencial y sólo se debe permitir el acceso a los dueños de la misma.

5.2. SERVICIO DE CORREO ELECTRÓNICO

Desde que un ingeniero llamado Ray Tomlison mandó el primer correo electrónico en 1971, los usuarios de Internet, entre los que probablemente te encuentras tú, se mandan unos a otros billones de mensajes de correo electrónico cada día. El servicio de correo electrónico fue el primero de los servicios que se desplegaron en Internet y, hoy en día, probablemente sea el servicio de mayor difusión después de la Web. ¿Te has preguntado alguna vez cómo llega un correo desde la aplicación de tu ordenador hasta el ordenador de tu amigo o amiga en el otro lado del mundo? En este apartado trataremos de dar respuesta a dicha pregunta. Veamos qué es y cómo funciona el correo electrónico.

Un correo electrónico o email, no es más que un simple mensaje de texto; es decir, un trozo de texto enviado a un destinatario. Los primeros sistemas de correo electrónico eran simples protocolos de transferencia de archivos de texto, con la convención de que la primera línea de cada archivo contenía la dirección del destinatario. De hecho, si bien es cierto que se ha producido cierta evolución para dar cierta estructura a los mensajes y a la manera de transmitirlos, éstos siguen estando compuestos exclusivamente por texto.

Una vez hecha la afirmación anterior, es probable que ahora mismo te estés haciendo la siguiente pregunta: si un correo está formado únicamente por texto, ¿cómo es que puedo enviar fotos u otros archivos a través del correo electrónico? Evidentemente, estos elementos no son texto; sin embargo, y al igual que sucedía en el protocolo HTTP, los protocolos para la transmisión de correo utilizan también mecanismos para codificar estos archivos en forma de

texto antes de ser transmitidos, y mecanismos para reconstruirlos a su forma original en el destino. Por eso, a todos los efectos, se puede afirmar que un correo electrónico está compuesto sólo por texto, aunque ciertos elementos no tengan esa naturaleza realmente.

El servicio de correo electrónico proporciona a los usuarios cinco funciones básicas:

- **Función de composición** - El sistema de correo electrónico debe permitir al usuario crear sus propios mensajes de correo y generar mensajes de respuesta a los correos recibidos.
- **Función de transferencia** - El sistema de correo electrónico tiene que mover los mensajes del emisor al destinatario y debe hacerlo automáticamente, sin molestar al usuario.
- **Función de generación de informe** - El sistema de correo debe indicar al remitente lo que ocurrió con el mensaje: ¿se entregó, se rechazó o se perdió?
- **Función de visualización** - El sistema de correo debe permitir al usuario ver y leer el contenido de los correos que le sean entregados.
- **Función de disposición** - El sistema de correo debe permitir al usuario decidir qué hacer con los correos entrantes tras recibirlos. Las posibilidades suelen incluir las de tirarlo antes de leerlo, desecharlo tras leerlo, guardarlo, etc. También debe permitir recuperar y releer mensajes previamente guardados, reenviarlos o procesarlos de otras maneras.

5.2.1. ARQUITECTURA DEL SERVICIO DE CORREO ELECTRÓNICO

Imagina que estás en tu ordenador preparado para enviar un correo electrónico a una persona. ¿Crees que será tu ordenador el que establezca directamente una comunicación con el ordenador del destinatario del correo para hacer la entrega del mismo? Reflexionemos sobre la pregunta anterior. Si eso fuese así, y para entregar un correo se estableciese una comunicación directa entre origen y destino del correo, ¿qué sucede si el ordenador del destinatario del correo estuviese apagado en el momento en el que queremos mandárselo? Evidentemente, montar un sistema de correo con estas bases no tiene mucho sentido. Pensemos en cómo funciona el sistema de correo tradicional, el que no es electrónico, el de toda la vida:

- Cuando queremos enviar una carta en el sistema de correo tradicional, ¿la llevamos nosotros mismos hasta su destinatario? Evidentemente no. Lo que hacemos es depositar nuestra carta en un buzón de correos público donde es recogida por un cartero. Entonces, el sistema de correos se encarga de hacerlo llegar hasta el destinatario.
- Cuando recibimos una carta, ¿nos lo entrega en mano el remitente del mismo? Evidentemente no. De hecho, ni siquiera el cartero nos la entrega en mano. Cada persona que quiere tener la capacidad de recibir correo tendrá un buzón privado

asignado. Entonces, lo que se hace es que el sistema de correos se compromete a depositar cualquier carta que vaya dirigida a nosotros en el buzón privado que nos pertenece. Nosotros, cuando queramos recoger nuestro correo, nos desplazaremos hasta nuestro buzón donde éste estará depositado.

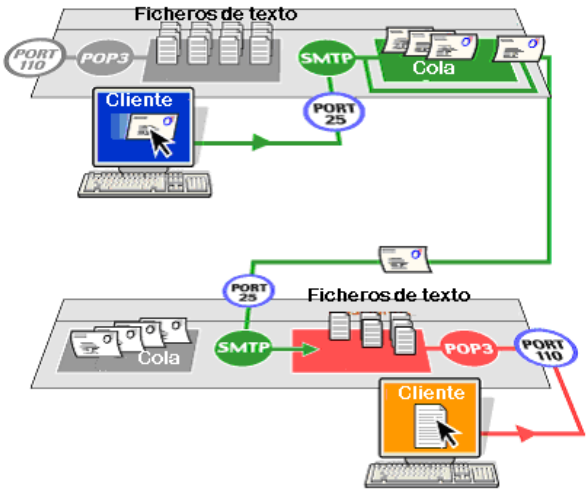
Pues bien, el sistema de correo electrónico sigue un esquema análogo a este sistema de correo tradicional. El servicio de correo electrónico sigue la filosofía cliente-servidor; sin embargo, su arquitectura es un poco más compleja que la de otros servicios de Internet. Como cualquier servicio que sigue este modelo, un sistema de correo electrónico está formado básicamente por dos elementos:

- **El cliente de correo o agente de usuario.**
- **El servidor de correo.**

Se llama clientes de correo o agentes de usuario a los programas utilizados por los usuarios finales y que les permiten leer, componer, recibir, contestar y enviar correo. Hoy en día tenemos a nuestra disposición multitud de clientes de correo, algunos tienen una interfaz gráfica elegante operada por menús y ventanas, mientras que otros tienen una interfaz textual en la que se introducen comandos desde el teclado. Aunque, evidentemente, para los usuarios son más atractivos y cómodos de utilizar los primeros, funcionalmente ambos son iguales.

Por su parte, el servidor de correo es una aplicación que tiene básicamente dos misiones o dos compromisos adquiridos con los usuarios a los que da servicio:

- **Mantener buzones para dichos usuarios y almacenar en ellos los correos que les van dirigidos** - Es decir, cualquier correo que vaya dirigido a un usuario, no será entregado directamente en el ordenador de éste, sino que será depositado en el buzón que su servidor de correo tiene para él. Además, evidentemente, un servidor de correo debe proporcionar algún mecanismo para que cada usuario pueda recoger sus correos de su respectivo buzón, acto que recibe el nombre coloquial de “descargarse el correo”.
- **Recoger los correos que los usuarios a los que da servicio le envían y encargarse de que éstos lleguen hasta el buzón del destinatario** - Es decir, cualquier correo que el usuario envía, no será entregado directamente al ordenador del destinatario, ni siquiera al servidor de correo del destinatario, sino al servidor de correo del emisor, el cual se encargará posteriormente de depositarlo en el buzón del destinatario, el cual estará alojado en el servidor de correo del mismo.



Un ordenador que hace de servidor de correo realmente está ejecutando dos aplicaciones servidoras diferentes:

- Una recibe el nombre de **servidor saliente** o **servidor SMTP**, cuyo puerto bien conocido es el **puerto 25**, y donde SMTP (**Simple Mail Transfer Protocolo**) o **Protocolo Simple para la Transmisión de Correo** es el nombre del protocolo que se utiliza para el envío de correo. Éste es el protocolo que utilizará el agente de usuario para entregar el mensaje a su servidor de correo, y también el que usará dicho servidor para entregar el correo al servidor en el que se encuentra el buzón del destinatario del mismo. Realmente, la entrega no tiene por qué ser directa desde el servidor de correo origen al servidor de correo destino, y el mensaje puede tener que pasar por distintos elementos intermedios. Tanto estos elementos intermedios como cualquier servidor de correo, reciben el nombre genérico de **MTA (Mail Transfer Agent) o Agentes de Transmisión de Correo**. El protocolo que utilizan los distintos Agentes de Transmisión de Correo para transferirse los mensajes es también el **protocolo SMTP**.
- La otra recibe el nombre de **servidor entrante** y tendrá la misión de gestionar la entrega del correo al usuario final al que va destinado; es decir, de permitir que un usuario pueda acceder a los mensajes que tiene almacenados en su buzón de su servidor de correo. Hay dos protocolos básicos que pueden ser utilizados para llevar a cabo esta tarea. Uno de ellos es el protocolo **POP3 (Post Office Protocol) o Protocolo de Oficina de Correos, versión 3**. El otro es el protocolo **IMAP (Internet Mail Access Protocol) o Protocolo para el Acceso al Correo Electrónico**. Según el protocolo que utilice el usuario para recuperar el correo de su buzón, el servidor entrante recibirá, respectivamente, el nombre de **servidor POP3, cuyo puerto bien conocido es el puerto 110, o el nombre de servidor IMAP, cuyo puerto bien conocido es el 143**.

5.2.2. DIRECCIONES DE CORREO ELECTRÓNICO

En el sistema de correos tradicional, ¿cómo sabe el cartero en qué buzones debe dejar las distintas cartas? Como bien conoces, el cartero puede realizar la entrega correctamente porque cada buzón tiene asociada una dirección que lo identifica unívocamente en todo el mundo. De igual manera, en Internet cada buzón de correo tiene asignada una dirección que lo identifica unívocamente en toda la Red. Para ello hay que localizar en la Red, por una parte, el ordenador en el que se encuentra el buzón buscado y, por otra, identificar el buzón entre los distintos buzones que haya alojados en el dicho ordenador. Toda dirección de correo electrónico está formada por las siguientes partes perfectamente diferenciadas:

- **Nombre del buzón de correo dentro del servidor**.
- **Un símbolo separador**, que se ha decidido que sea la arroba: @.
- **El nombre DNS del ordenador en el que se encuentra la aplicación servidor de correo**.

EJEMPLO

Direcciones de correo electrónico:

- antonio@gmail.com
- pedrolopez@jgpa.es
- jose@hotmail.com

5.2.3. FORMATO DE UN MENSAJE DE CORREO ELECTRÓNICO

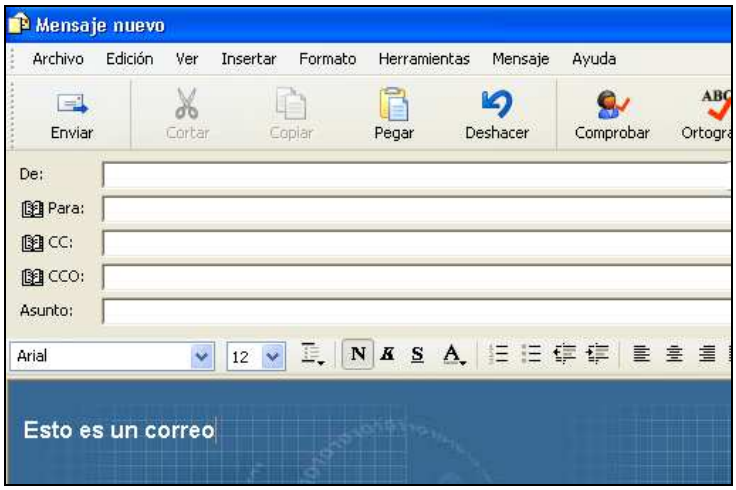
Una vez descrita la arquitectura de un sistema de correo, es hora de describir el formato de un mensaje en sí, pues igual que para poder mandar una carta por el sistema de correo tradicional hay que seguir ciertas convenciones que establecen, por ejemplo, qué hay que poner en el sobre y cómo ponerlo, en el sistema de correo electrónico los mensajes deben ajustarse a un formato establecido. En todo mensaje de correo podemos distinguir las siguientes partes:

- **La envoltura primitiva** - la cual **encapsula al mensaje y contiene toda la información que necesitan los agentes de transferencia de correo (MTA)** para poder transportarlo desde el servidor origen hasta el servidor destino. Es decir, podemos afirmar que la envoltura de un mensaje juega el mismo papel que juega el sobre en el sistema de correo tradicional. **Los usuarios finales no son conscientes de la existencia de esta envoltura** pues la misma sólo es manejada por los agentes de transferencia de correo; de hecho, es creada en el servidor de correo origen y es eliminada por el servidor de correo del destinatario antes de depositar el mensaje en el buzón.
- **Cabecera del mensaje** - Dentro de lo que es el mensaje en sí, **la cabecera es la parte que contiene información de control para los clientes de correo**. Está información está formado por un número variable de campos, si bien es cierto que hay una serie de campos que son obligatorios, y cada uno de ellos sigue el formato "nombre_del_campo:valor_del_campo".
- **Cuerpo del mensaje** - Dentro de lo que es el mensaje en sí, se llama cuerpo del mensaje a la parte del mismo que va dirigido al destinatario humano; es decir, **la carta en sí misma**.

De entre los numerosos campos que pueden aparecer en la cabecera del mensaje cabe destacar los siguientes:

- **Campo To** - Campo de presencia obligatoria que contiene las direcciones de correo de los destinatarios del mensaje, también llamados **destinatarios primarios**.
- **Campo From** - Campo de presencia obligatoria que informa de quién es el remitente del mensaje.
- **Campo CC** o campo de copia al carbón - Campo que contiene las direcciones de correo de aquellos destinatarios del mensaje a los que, aunque el correo no va dirigido a ellos, se les quiere mandar una copia del mismo. Éstos reciben el nombre de **destinatarios secundarios** y, en términos de entrega, no hay diferencia entre ellos y los destinatarios primarios. Es una diferencia por entero psicológica que puede ser importante para los participantes, pero que no lo es para el sistema de correo.
- **Campo BCC** o campo de copia de carbón ciega - Campo similar al campo CC, excepto que esta línea se borra de todas las copias enviadas a los destinatarios primarios y secundarios. Esta característica **permite a la gente mandar copias a terceros sin que los destinatarios primarios y secundarios lo sepan**.
- **Campo Subject** - Campo que contiene un resumen corto del mensaje para exhibir en una línea.
- **Campo Date** - Campo que contiene la fecha y hora del envío del mensaje.

- **Campo Reply-To** - Campo que contiene la dirección de correo a la que deben enviarse las contestaciones al mismo. Generalmente contiene el mismo valor que el campo From, pero no tiene por qué ser así. Imagina un encargado de marketing que manda un mensaje a los clientes de la empresa para informarles sobre la aparición de un producto nuevo. Los clientes deben contestar a dicho correo para solicitar sus pedidos; sin embargo, dichas contestaciones deberán llegar al jefe de ventas. Por lo tanto, el campo From contendrá la dirección del empleado de marketing, mientras que el campo Reply-To contendrá la dirección del jefe de ventas.



5.2.4. SEGURIDAD EN EL CORREO ELECTRÓNICO

Cuando mandas una carta, ¿te preocupa la posibilidad de que ésta sea leída por el camino por alguna otra persona a la que no iba dirigida? ¿Tenemos derecho como ciudadanos a que esto no suceda? El artículo 18 de la Constitución Española de 1978 establece en su punto tercero que: “se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial” y en su punto cuarto que: “la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

La seguridad y fiabilidad que nos proporciona el correo tradicional la conocemos y la tenemos asumida, pero ¿qué sucede con el correo electrónico? ¿Qué seguridad tengo de que un correo electrónico que envío sólo será leído por su destinatario? En principio, ninguna. Cuando mandamos un correo electrónico a través de la red, estamos mandándolo sin protección alguna. Es como si mandásemos una postal. Cualquier persona que intercepte dicho correo (durante la transmisión, una vez en el buzón o en el propio equipo del usuario destino) podrá extraer y examinar su contenido. Además, es posible incluso que éste sea modificado por el camino sin que ni siquiera emisor ni receptor se dé cuenta. Evidentemente, esta situación es intolerable. ¿Hay alguna manera de evitarlo?

Muchos servidores de correo ofrecen la posibilidad de utilizar protocolos seguros para la transmisión del correo entre el cliente de correo y el servidor, ya sea en el proceso de envío de mensajes o en el proceso de recogida de correo desde el buzón. Estos

protocolos siguen siendo SMTP y POP3 o IMAP, pero utilizando **protocolos de cifrado**, como **SSL o TLS**, antes de enviar la información. El uso de estos protocolos asegura:

- Que si el correo es interceptado durante la transmisión entre cliente de correo y servidor de correo no podrá ser leído.
- Que el correo no podrá ser modificado durante la transmisión entre cliente de correo y servidor.

Sin embargo, esto no es suficiente para garantizar la completa privacidad del correo, porque:

- ¿Qué sucede durante el trasiego del correo por todos los MTA hasta llegar al destino? Pues los protocolos mencionados antes no cubren este trayecto.
- ¿Qué sucede una vez que el correo está depositado en el buzón del destinatario? ¿Puede alguien fisgar en el buzón?
- ¿Qué sucede una vez que el correo está en el ordenador del destinatario? ¿Puede alguien fisgar en su ordenador y leer su correo?

Evidentemente, con el uso de los protocolos descritos no estamos protegidos ante estas eventualidades descritas. Para garantizar de manera total la seguridad en las comunicaciones por correo electrónico, debemos recurrir a sistemas criptográficos extremo a extremo; es decir, establecidos entre la persona emisora del correo y la persona receptora del mismo. Uno de estos sistemas es **PGP** (Pretty Good Privacy) o **Privacidad Bastante Buena**, el cual es un sistema de criptografía gratuito para aplicaciones no comerciales.

5.3. SERVICIO DE TRANSFERENCIA DE FICHEROS

Otro de los servicios que nos acompañan desde la aparición de Internet es el **protocolo FTP (File Transfer Protocol) o Protocolo para la Transferencia de Ficheros,** que permite a los usuarios copiar archivos entre sistemas remotos. FTP comenzó siendo una utilidad incluida en el sistema operativo Unix en los años 70 y, si bien al principio éste era un protocolo muy usado, ahora, con la aparición de aplicaciones Web que permiten la subida y descarga de ficheros usando HTTP.

Parece que el FTP está un poco más en desuso, por lo menos por parte del gran público. No obstante, sigue siendo uno de los servicios fuertes de Internet y de los más importantes.

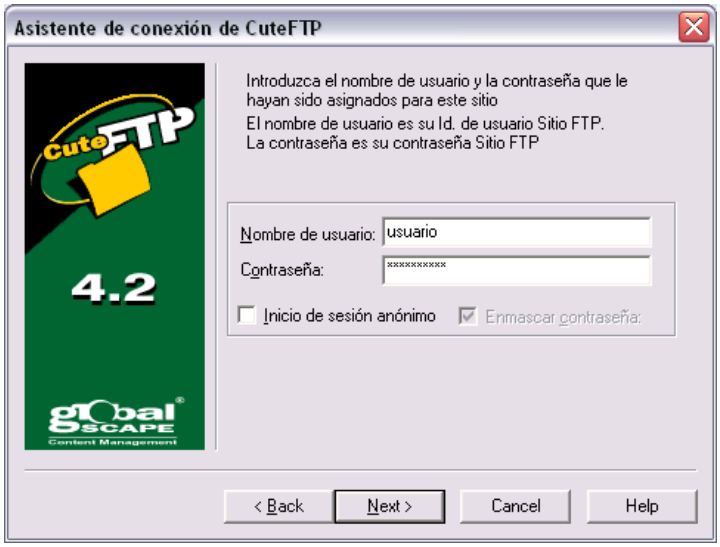
Al igual que los anteriores servicios, **el servicio FTP también sigue la filosofía cliente-servidor**. Esto quiere decir que en la comunicación existirán dos tipos de aplicaciones implicadas:

- **El servidor FTP** - Es la aplicación que proporciona el servicio de proporcionar un espacio de disco en el que se puedan dejar archivos o desde el que se puedan recoger archivos.
- **El cliente FTP** - Es la aplicación que permite a un usuario conectarse a un servidor FTP para poder dejar en él algún archivo o para poder descargar de él algún archivo.

Por tanto, el protocolo FTP es un protocolo de aplicación apto para la transferencia fiable de archivos en ambos sentidos entre una aplicación servidora de FTP y una aplicación cliente de FTP, cuyas funciones esenciales permiten a los usuarios realizar tareas básicas como copiar, mover, renombrar y trabajar con ficheros y directorios de forma remota.

Normalmente, un servidor FTP se configura para autentificar los inicios de sesión de los clientes, pidiendo la identificación de los mismos mediante un nombre de usuario y una contraseña, llamados login y password respectivamente, antes de acceder al sistema. Sin embargo, esta autentificación no es obligatoria siempre. FTP tiene dos modalidades de uso:

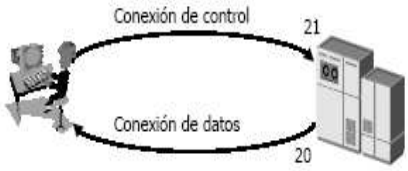
- **FTP Anónimo** - Esto supone un servidor **FTP configurado para permitir el acceso público**, es decir, el sistema se ajusta a una clave de acceso público para permitir el acceso anónimo a todos los archivos que se han compartido. Generalmente, este servicio se utiliza para mantener información y software de libre acceso a todo el mundo. En unas ocasiones sólo se pueden descargar ficheros, y en otras éstos se pueden tanto subir como bajar.
- **FTP Privado** - En este caso **el servidor se basa en autentificación a partir de la base de datos de usuarios locales**, por lo tanto, sólo pueden iniciar sesión los usuarios que hayan sido dados de alta en dicho sistema. Normalmente este tipo de FTP es utilizado por compañías que requieren de acceso remoto o en entornos donde la información es confidencial.



Cuando se establece una sesión FTP entre un cliente y un servidor, realmente se establecen dos conexiones con el servidor:

- Una **conexión de control** - Que es iniciada por la aplicación cliente para la transmisión de comandos a través del **puerto 21 del servidor**, y que es mantenida durante toda la sesión
- Una **conexión de datos** - Que es iniciada por la aplicación servidora para la transmisión de datos, y que se abre y se cierra por archivo a enviar o recibir. Cada

una de estas conexiones temporales **se abre desde el puerto 20 del servidor contra un puerto cualquiera del cliente que éste le haya comunicado previamente.**



Aunque el protocolo FTP establece mecanismos para la autenticación de usuarios mediante login y password, éstos así como los ficheros transmitidos entre cliente y servidor viajan en claro por la red; es decir, que pueden ser interceptados y leídos por el camino, hecho por el cual **se considera FTP un protocolo no seguro**.

5.4. SERVICIO DE CONEXIÓN REMOTA

Cuando nosotros, como usuarios, queremos trabajar con el ordenador, nos sentamos ante nuestro teclado, nuestro ratón y nuestra pantalla, pulsamos el botón de encendido del ordenador y nos ponemos manos a la obra. Con este sencillo gesto, lo que realmente estamos haciendo es abrir lo que se llama una sesión con el sistema operativo, con el cual interactuamos para llevar a cabo nuestra labor. La pregunta que vamos a plantearnos y a dar respuesta, ahora que ya vamos siendo conscientes de la potencia de las redes de ordenadores, es la siguiente: ¿es posible iniciar una sesión desde mi ordenador y a través de la red en un ordenador remoto? Es decir, ¿es posible trabajar en un ordenador con el que no comparto un espacio físico, como si estuviese sentado delante del mismo? La respuesta es, evidentemente, que sí, gracias a unos servicios de red conocidos con el nombre de servicios de conexión remota.

Al igual que el resto de servicios analizados, **los servicios de conexión remota siguen la filosofía cliente-servidor**. Esto quiere decir que en la comunicación existirán dos tipos de aplicaciones implicadas:

- **El servidor** - El cual es, desde el punto de vista del usuario del servicio, el ordenador remoto en el cual se abre la sesión del sistema operativo y sobre el cual se trabaja.
- **El cliente** - El cual es, desde el punto de vista del usuario, el ordenador local desde el cual se abre la sesión en el ordenador remoto.

Básicamente, un servicio de conexión remota funciona de la siguiente forma:

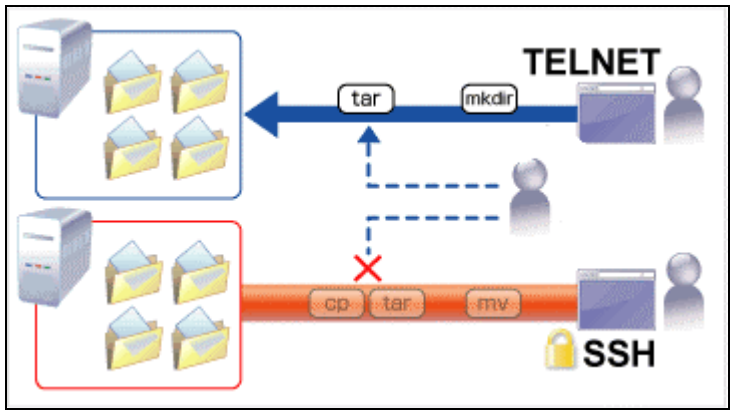
- Un usuario inicia una sesión en su propio ordenador.
- El usuario ejecuta en su ordenador un programa cliente de conexión remota.
- Con dicho programa se conecta a un servidor remoto, en el cual abre una conexión remota.

- Una vez abierta la sesión remota, y través de su aplicación cliente, el usuario ve en su pantalla local lo mismo que vería si estuviese sentado delante del ordenador remoto.
- Conforme el usuario interactúa con su aplicación cliente, ésta envía la información de dicha interacción, como pulsaciones de teclas del teclado o movimientos del ratón, al servidor.
- El servidor recibe dicha información desde el cliente y le devuelve a éste los resultados que la interacción ha provocado en el sistema.

Por tanto, la sensación que percibe el usuario es que la sesión remota tiene lugar en la computadora local, mientras que el equipo remoto "piensa" que está interactuando con un terminal local; es decir, con una persona sentada delante del teclado, ratón y monitor local.

Antes de la aparición de los sistemas operativos gráficos que cuentan con ventanas, botones, menús, etc., la manera de interactuar con un sistema operativo era con la utilización de comandos que se introducían desde una consola de texto; es decir, una pantalla negra donde únicamente se podía introducir órdenes en forma de texto desde el teclado. Según si la conexión remota se va a abrir contra una aplicación servidora textual o gráfica, podemos distinguir dos tipos de servicios:

- Conexión remota con terminal de comandos.
- Conexión remota con terminal gráfico.



Dentro de los protocolos de aplicación para la realización del servicio de conexión remota, **cabe destacar el protocolo originario, llamado Telnet, que es un protocolo para la conexión remota con terminal de comandos**. Sin embargo, en dicho protocolo la información que intercambian cliente y servidor viaja en claro por la red, lo que quiere decir que puede ser interceptada y leída por el camino. Por este motivo, **el protocolo Telnet, aunque establece mecanismos para la autenticación del usuario que quiere abrir la sesión mediante el requerimiento de un login y un password, es considerado un protocolo no seguro**. Por otra parte, **existe otro protocolo muy parecido que sí es seguro, pues utiliza técnicas de cifrado para que la información que viaja por la red no pueda ser leída por nadie al que**

no vaya dirigida. Dicho protocolo es el **protocolo SSH (Secure shell) o terminal de comandos seguro**.

6. MECANISMOS DE SEGURIDAD BÁSICOS EN INTERNET

Sobre la seguridad de un sistema informático, Gene Spafford, profesor de la Universidad de Purdue y reconocido científico especializado en temas de seguridad informática, afirmó un día: "el único sistema auténticamente seguro es el que está desconectado, desenchufado y empaquetado en un recipiente hermético de titanio y guardado en un bunker de hormigón. E incluso así, yo no me jugaría la vida por él". Si el señor Spafford tenía sus dudas sobre la seguridad de un sistema en las condiciones anteriormente descritas, ¿qué no pensará de un ordenador conectado a Internet?

Cuando pensamos en tomar medidas de seguridad en nuestro ordenador, lo primero que se nos viene a la cabeza como principal peligro del que debemos protegernos son los virus. Todos los días escuchamos en las noticias la aparición de nuevas formas de estos programas malignos. Pero, ¿qué es exactamente un virus? Un virus es un programa cuyo objetivo prioritario es su propagación entre ordenadores sin ser advertido por el usuario. Una vez que el virus considera que está lo suficientemente extendido, pasa de su fase de latencia a su fase de activación. En esta fase los efectos del virus pueden ser tan variados como alcance la imaginación de su autor: pueden limitarse a mostrar inofensivos mensajes en pantalla o bien, eliminar información del disco duro o dañar la BIOS del ordenador.

Las vías clásicas de propagación de los virus han sido siempre los disquetes, CD-ROMs, discos ZIP, etc. Sin embargo, con la aparición de Internet, las estadísticas demuestran que la principal vía de infección de virus son las redes de ordenadores, y dentro de los servicios que ésta ofrece, el favorito usado por los virus para su propagación es el correo electrónico. Los virus viajan en mensajes de correo como ficheros adjuntos al mensaje y si el receptor del mismo abre dicho archivo, su ordenador queda inmediatamente infectado. Además, una vez conseguida la infección del equipo, el virus, se reenvía automáticamente a través del correo a todas las direcciones de correo que encuentre en la libreta de direcciones del cliente de correo del usuario infectado.

Los virus han evolucionado mucho desde sus orígenes. De entre las nuevas modalidades de virus, distinguimos las dos siguientes:

- **Los gusanos** - Se llama gusanos a los virus que usan para replicarse las redes de ordenadores y los agujeros de seguridad de los programas instalados en los ordenadores de las mismas. Una vez que un virus gusano ha infectado un ordenador, estudia la red en busca de alguna otra máquina que tenga instalado y funcionando el software que tiene el agujero de seguridad que dicho gusano explota. Entonces, se copia vuelve a copiar a sí mismo en el nuevo ordenador y comienza de nuevo su proceso de réplica.

- **Los caballos de Troya** - Un caballo de Troya es un programa que tiene una apariencia inofensiva pero que realmente tiene objetivos hostiles. En concreto, se trata de un programa con dos módulos: un módulo servidor y otro cliente. El atacante se instala, con fines nada éticos, el módulo cliente en su ordenador. El módulo servidor es el troyano propiamente dicho, que se envía a la víctima bajo alguna apariencia completamente inofensiva, por ejemplo, unas fotos, un juego, etc. Una vez que la víctima cae en la trampa y ejecuta el archivo éste se instala en su ordenador. A partir de ese momento, el atacante puede monitorizar todo lo que la víctima hace en su ordenador incluyendo el robo de contraseñas y documentos privados. El troyano, después de ejecutarse, abre un determinado puerto en modo escucha en el ordenador de la víctima. El atacante puede crear entonces una conexión desde su ordenador hasta la dirección IP y puerto de la víctima (debe conocer estos dos números o diseñar algún método para obtenerlos). Una vez que está establecida la conexión, el atacante, que puede estar a miles de kilómetros, tendrá acceso completo al ordenador de la víctima.

6.1. PROTEGER NUESTROS ORDENADORES DE LOS VIRUS

¿Cómo podemos proteger nuestros ordenadores de los virus? Básicamente deberemos dirigir nuestras actuaciones por dos frentes distintos:

- **Mediante el uso de programas antivirus** - los cuales detectan la presencia de virus en archivos impidiendo la infección del sistema. Además, disponen de rutinas de desinfección que tendrán mayor o menor éxito en función del tipo de virus y de la calidad del propio programa antivirus. No obstante, debemos tener en mente que los programas antivirus no son una solución infalible: cada día se desarrollan nuevos virus los cuales pueden no ser detectados por nuestro programa antivirus. Por eso es imprescindible tener un programa antivirus permanentemente actualizado, de tal manera que sea capaz de detectar los últimos virus aparecidos. Sin embargo, como decimos, un antivirus no es una solución infalible. Las desinfecciones de archivos en caso de que un posible virus haya destruido datos, sobrescribiéndolos con caracteres basura, por ejemplo, pueden no tener ningún éxito. Además, en la mayoría de los casos, después de una infección, no queda más remedio que reinstalar equipos y recuperar datos de copias de seguridad. Por lo tanto, debemos invertir en medidas de prevención y detección para que las infecciones no lleguen a producirse. Si a pesar de todo ocurre lo peor, debemos contar con copias de seguridad que hagan que las consecuencias sean las menores posibles
- **Mediante una adecuada formación de los usuarios** - Si los usuarios de los ordenadores son conscientes de qué acciones pueden comportar algún peligro, saben qué no deben hacer y toman una serie de precauciones de seguridad y protección, gran parte de las infecciones pueden ser evitadas. De hecho, al igual que en la vida real, las medidas preventivas suelen ser las medidas más eficientes,

puesto que resultan efectivas tanto con virus conocidos como desconocidos. Así, por ejemplo, los usuarios deben saber que no deben abrir archivos ejecutables que vengan adjuntos en el correo electrónico, deben saber que ciertos documentos de aplicaciones ofimáticas pueden contener virus de macro y deben ser comprobados con programas antivirus antes de abrirlos, etc.

Pero estas dos medidas descritas puede que no sean suficientes para estar completamente protegidos. Así, por ejemplo, los antivirus no son los programas más efectivos para enfrentarse a los caballos de Troya. En su lugar, es más recomendable la utilización de un firewall o cortafuegos, ya que éstos pueden impedir que una aplicación de este tipo se comunique a través de la red.

¿Has viajado alguna vez a algún país no perteneciente a la Unión Europea? Si es así, seguro que has pasado alguna vez por un control de aduanas y sabrás que su tarea es la de examinar a fondo a todo aquél que quiere cruzarla, ya sea en un sentido o en otro, preguntar qué intenciones tiene y, en función de eso, decidir quién puede pasar la aduana y quién no. En definitiva, lo que pretenden los países con las aduanas es dotarse de ciertos mecanismos de seguridad.

6.2. CORTAFUEGOS (≅ FIREWALL)

Un cortafuegos es una herramienta hardware o software utilizada en las redes de ordenadores con el objetivo de dotar de cierta seguridad a las mismas. Podemos pensar en un firewall como si fuese un control de aduanas a través del cual tiene que pasar todo el tráfico IP que circula por la red. Al igual que en un control de aduanas, en este punto se tomará la decisión de qué paquete IP puede seguir su curso y qué paquete IP es detenido y destruido. Como sabemos, en una aduana, la decisión de si una persona puede pasar o no se toma en función de quién es esa persona, qué actividades va a desarrollar en el país al que entra, etc. De igual modo, en un cortafuegos, la decisión de si un paquete IP puede pasar el firewall o no se tomará en función de las direcciones IP origen y/o destino de dicho paquete, así como del puerto origen y/o destino al que vaya dirigida la información que dicho paquete transporta. Así, por ejemplo, con un firewall:

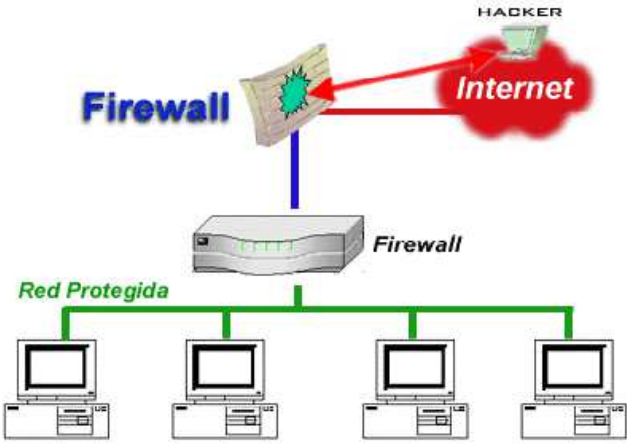
- Se puede impedir el paso a todo el tráfico IP que vaya dirigido a una cierta dirección IP o a una red concreta.
- Se puede impedir el paso a todo el tráfico que provenga de cierta dirección IP o de cierta red concreta.
- Se puede impedir el paso a todo tráfico que no provenga de cierta dirección IP o de cierta red concreta o que no vaya dirigido a cierta dirección IP o a cierta red concreta.
- Se puede impedir el paso del tráfico que vaya dirigido a un puerto concreto, por ejemplo, al puerto 80, con lo que cerraríamos el tráfico de acceso a la Web.

- Se puede permitir el acceso al puerto 80 de ciertos ordenadores e impedir el acceso al puerto 80 de otros ordenadores, con lo que estableceríamos a qué servidores Web nos podemos conectar y a cuáles no.
- Se puede, en definitiva, hacer cualquier combinación de criterios que juegue con direcciones IP origen y destino de los paquetes y puertos origen y destino de la información que transportan.

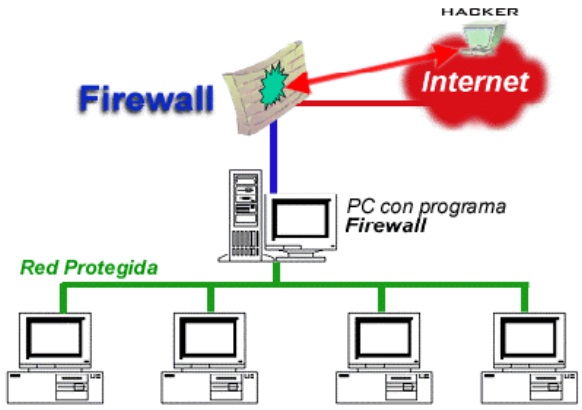
6.2.1. TIPOS DE CORTAFUEGOS

Según el lugar en el que estén situados, podemos distinguir dos tipos de firewall:

- **Cortafuegos corporativos** - Es un firewall hardware o software situado en el router de salida o entrada de una red local y cuyo objetivo es el de dar protección a la misma, controlando qué tráfico puede salir y entrar desde y hacia la red.



- **Cortafuegos personales** - Es un firewall software situado en un ordenador personal y cuyo objetivo es el de dar protección al mismo, controlando qué tráfico puede salir del ordenador hacia la red y qué tráfico puede entrar desde la red hacia el ordenador. Este software avisará al usuario cuando detecte el establecimiento de una conexión sospechosa o simplemente la rechazará. Este tipo de cortafuegos cuenta con la peculiaridad de que, además de filtrar el tráfico por dirección IP y puertos, también permite al usuario establecer los permisos en función de las aplicaciones, decidiendo qué programas pueden comunicarse por la red y cuál no. Esto acerca una herramienta de este tipo a los usuarios sin conocimientos en informática.



Como hemos visto, son muchos los peligros que acechan en la Red y es prácticamente imposible ponerse totalmente a salvo de todos ellos. El mejor consejo, no volverse paranoico, pero tampoco dejado. Lo más recomendable es llegar a un compromiso esfuerzo/necesidad; es decir, tener muy claro qué hay que proteger y qué no, valorar la importancia y las necesidades de seguridad en cada caso, y realizar una inversión acorde a esas necesidades particulares. No obstante, hay una serie de normas básicas que debemos seguir para tener unas garantías mínimas de seguridad:

- Contar con software completamente actualizado, tanto el sistema operativo como las aplicaciones instaladas, pues muchos de los ataques a la seguridad aprovechan vulnerabilidades, agujeros o errores del software instalado en el equipo, los cuales suelen ser corregidos en versiones superiores de los programas.
- Disponer de un antivirus actualizado que nos ayude a combatir los distintos tipos de software maligno que puede de alguna manera infectar nuestro ordenador.
- Disponer de un firewall que nos permita controlar los accesos a la red.
- Guardar copias de seguridad de los datos importantes y críticos, para que, en caso de catástrofe, no los perdamos.

6.3. PROXY

Pero no todas las medidas que tomamos cuando nos conectamos a Internet están orientadas a la seguridad, sino que hay otras muchas orientadas al control. ¿Tienes hijos pequeños? Si es así, ¿a qué te gustaría poder impedirles el acceso a ciertas páginas Web de contenido no apropiado? De igual manera, al dueño de una empresa le puede interesar impedir que un trabajador se dedique a leer la prensa digital durante su horario de trabajo. Como hemos visto, un cortafuegos no es capaz de precisar tanto filtrando, pues nos permitiría, por ejemplo, cortar todo el tráfico Web, pero no el tráfico sólo a ciertas páginas. ¿Es posible ejercer un control tan afinado? La respuesta es que sí, haciendo uso de lo que se conoce como **servidor proxy, en este caso un servidor proxy HTTP**.

Un servidor proxy HTTP es una aplicación que se sitúa entre el navegador y el servidor Web de tal manera que intercepta las conexiones HTTP de aquél y lo sustituye de cara al servidor. Al pasar todas las conexiones HTTP a través de esta aplicación, se pueden establecer en ella ciertos criterios de filtrado para controlar, en función de la URL solicitada, qué conexiones HTTP están permitidas y cuáles no. Así, por ejemplo:

- Se pueden impedir las conexiones a ciertas URLs, explicitando cuáles deben ser restringidas.
- Se puede afinar aún más en este aspecto, impidiendo las conexiones a URLs que contengan alguna palabra clave, por ejemplo, la palabra sexo.
- Se puede impedir la descarga de recursos de un cierto tipo, por ejemplo, fotos o ficheros musicales.

Generalmente el servidor proxy HTTP se sitúa, al igual que el cortafuegos, en el router de salida de la red y monitoriza de forma transparente para el usuario (es decir, sin que éste se dé cuenta) sus conexiones Web hacia el exterior de la red local. Además de restringir las conexiones HTTP de los usuarios, con un proxy HTTP, también podemos realizar las siguientes acciones:

- Se puede mantener un registro de quién está navegando por la Web, cuándo se conecta y dónde se conecta.
- Se pueden establecer horas en las que la conexión esté permitida y horas a las que no.
- Se pueden especificar distintas políticas de uso de la Web, de tal manera que unos usuarios tengan unas restricciones y otros usuarios tengan otras o ninguna.
- Se puede acelerar el acceso a la Web mediante el uso de una caché en el servidor proxy. Si está opción de configuración del servidor proxy está disponible y activada, el servidor mantendrá una copia de las páginas solicitadas, de tal manera que, si vuelven a ser pedidas posteriormente, por el mismo o por otro usuario, éstas pueden ser servidas por el proxy en vez de por el servidor que aloja dichas páginas realmente, lo cual se traduce en una mayor rapidez de servicio.

- Se puede compartir la conexión a Internet para la navegación Web. Si sólo tiene conexión a Internet un único ordenador, por ejemplo, mediante una conexión ADSL, el resto de ordenadores de la red local pueden navegar por la Web a través de él si dicho ordenador cuenta con una aplicación proxy HTTP que los sustituya en las conexiones.