Tema 7: Servicios en red.

1. Elementos de la arquitectura cliente/servidor.

De lo dicho hasta ahora, podemos deducir que los principales elementos que conforman la arquitectura cliente/servidor son los siguientes:

1.1. El servidor.

Cuando hablamos de una forma genérica, al mencionar a un servidor, nos referimos a un ordenador, normalmente con prestaciones elevadas, que ejecuta servicios para atender las demandas de diferentes clientes.

Sin embargo, bajo el punto de vista de la arquitectura cliente/servidor, un servidor es un proceso que ofrece el recurso (o recursos) a los clientes que lo solicitan (consultar la definición de cliente más abajo).

Es muy frecuente que, para referirse a un proceso servidor, se utilice el término back-end.

Por último, mencionar que, en algunas ocasiones, un servidor puede actuar, a su vez, como cliente de otro servidor.

1.2. El cliente.

Igual que antes, al hablar de forma genérica sobre un cliente, nos referimos a un ordenador, normalmente con prestaciones ajustadas, que requiere los servicios de un equipo servidor.

Sin embargo, bajo el punto de vista de la arquitectura cliente/servidor, un cliente es un proceso que solicita los servicios de otro, normalmente a petición de un usuario.

En entornos cliente/servidor, suele utilizarse el término front-end para referirse a un proceso cliente.

Normalmente, un proceso cliente se encarga de interactuar con el usuario, por lo que estará construido con alguna herramienta que permita implementar interfaces gráficas (o GUI, del inglés graphical user interface). Además, se encargará de formular las solicitudes al servidor y recibir su respuesta, por lo que deberá encargarse de una parte de la lógica de la aplicación y de realizar algunas validaciones de forma local.

1.3. El Middleware.

Es la parte del software del sistema que se encarga del transporte de los mensajes entre el cliente y el servidor, por lo que se ejecuta en ambos lados de la estructura.

El middleware permite independizar a los clientes y a los servidores, sobre todo, gracias a los sistemas abiertos, que eliminan la necesidad de supeditarse a tecnologías propietarias.

Por lo tanto, el middleware facilita el desarrollo de aplicaciones, porque resuelve la parte del transporte de mensajes y facilita la interconexión de sistemas heterogéneos sin utilizar tecnologías propietarias.

Además, ofrece más control sobre el negocio, debido a que permite obtener información desde diferentes orígenes (uniendo tecnologías y arquitecturas distintas) y ofrecerla de manera conjunta.

Podemos estructurar el middleware en tres niveles:

- El protocolo de transporte, que será común para otras aplicaciones del sistema.
- El sistema operativo de red.
- El protocolo del servicio, que será específico del tipo de sistema cliente/servidor que estemos considerando.

Para dar respuesta a estas situaciones, estableceremos dos tipos de clasificación diferentes: El primero atenderá al tamaño del lado servidor comparado con el tamaño del lado cliente. El segundo hará referencia al tipo de servicio que se ofrece.

1.4. El funcionamiento básico.

Aunque se menciona en temas pasados, repetimos el funcionamiento general del modelo cliente/servidor:

Lo primero que debe ocurrir es que se inicie el servidor. Esto ocurrirá durante el arranque del sistema operativo o con la intervención posterior del administrador del sistema. Cuando termine de iniciarse, esperará de forma pasiva las solicitudes de los clientes.

En algún momento, uno de los clientes conectados al sistema realizará una solicitud al servidor.

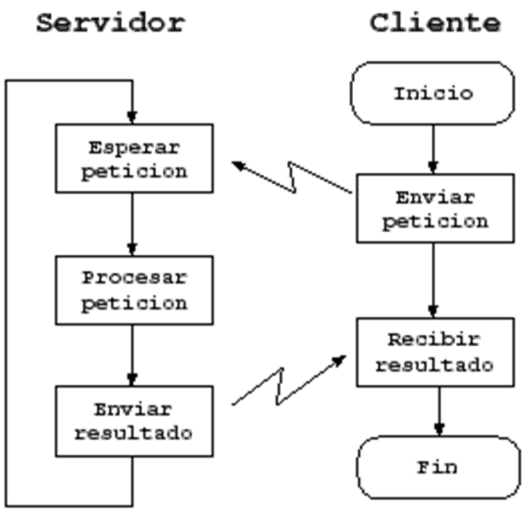
El servidor recibe la solicitud del cliente, realiza cualquier verificación necesaria y, si todo es correcto, la procesa.

Cuando el servidor disponga del resultado solicitado, lo envía al cliente.

Finalmente, el cliente recibe el resultado que solicitó. A continuación, realiza las comprobaciones oportunas (si son necesarias) y, si era ese el objetivo final, se lo muestra al usuario.

Clasificación según el tamaño del lado cliente y del lado servidor

Una de las características del modelo cliente/servidor es que permite balancear la potencia de cálculo aplicada hacia el lado servidor o hacia el lado cliente, según convenga.



2. Seguridad.

Uno de los aspectos más importantes a la hora de asegurar la red correctamente es la arquitectura de red. Una arquitectura de red es el diseño de la red en el que se emplean unos determinados componentes, cuya finalidad es la de canalizar, permitir o denegar el tráfico con los elementos apropiados.

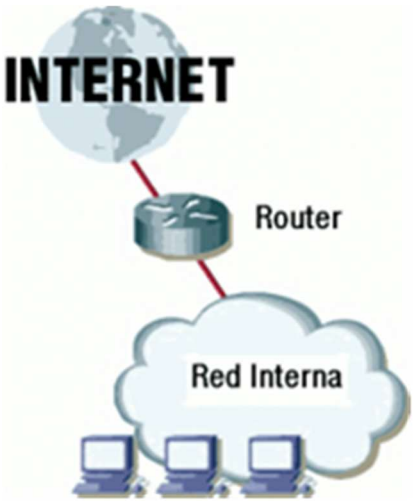
Existen varias arquitecturas de red, desde la más sencilla, que utiliza simplemente un router, hasta otras más complejas, basadas en varios routers, proxys y redes perimetrales (o zonas neutras).

Antes de entrar en detalle con las arquitecturas de cortafuegos se van a describir tres elementos básicos que intervienen en ella:

- **Router**. Equipo que permite o deniega las comunicaciones entre dos o más redes. Al ser el intermediario entre varias redes debe estar especialmente protegido ya que puede ser objeto de un ataque. Un router puede ser un dispositivo específico o un servidor que actúe como router.
- **Red interna**. Es la red interna de la empresa y, por lo tanto, es donde se encuentran los equipos y servidores internos. Dependiendo del nivel de seguridad que necesite la red interna se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra.
- **Zona neutra (O red perimetral).** Red añadida entre dos redes para proporcionar mayor protección a una de ellas. En esta red suelen estar ubicados los servidores de la empresa. Su principal objetivo es que ante una posible intrusión en unos de los servidores, se aísle la intrusión y no se permita el acceso a la red interna de la empresa.

A continuación, se va a ver el esquema de red básico que se puede utilizar cuando desea crear una red interna pero no hay servidores que ofrezcan servicios a Internet. En el caso de tener servidores públicos entonces se recomienda tener una zona neutra.

A partir del esquema de red con una zona neutra se pueden realizar todas las modificaciones que estimes oportunas dependiendo de la seguridad que quieras tener en la red interna, si quieres más zonas neutras, varias conexiones a Internet, etcétera. En este caso lo importante es adaptar el esquema de red a las necesidades de la empresa.



2.1. Esquema de red básico.

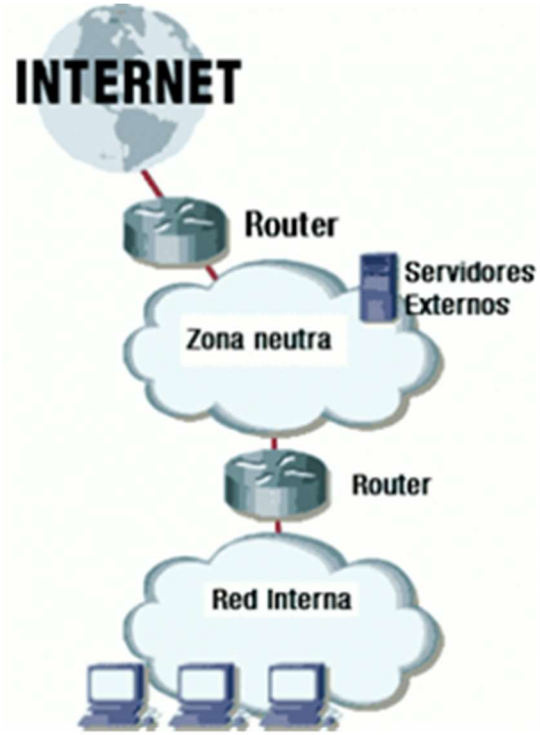
Es la configuración más simple y consiste en el empleo de un router para comunicar la red interna de la empresa con Internet. Como el router es el encargado de comunicar ambas redes es ideal para permitir o denegar el tráfico.

Esta arquitectura de red, aunque es la más sencilla de configurar es la más insegura de todas ya que toda la seguridad reside en un único punto: el router. En caso de que se produzca un fallo de seguridad en el router el atacante tiene acceso a toda la red interna.

Otro aspecto muy importante es que si se desea tener un servidor que ofrezca servicios a Internet hay que ubicarlo en la red interna. Es peligroso poner el servidor en la red interna ya que el router permite el tráfico al servidor y, en el caso de que se produzca un fallo de seguridad el atacante tiene acceso completo a la red interna. Para solucionar este problema se añade una nueva red a la empresa que se denomina **zona neutra o zona desmilitarizada.**

2.2. Esquema de red con una zona neutra.

Este esquema de red es considerado como el esquema base cuando quiere ofrecer servicios a Internet manteniendo un nivel adecuado de seguridad en la red interna. Como puede ver en la siguiente figura, esta arquitectura utiliza dos routers que permiten crear un perímetro de seguridad (red perimetral o zona neutra), en la que se pueden ubicar los servidores accesibles desde el exterior, protegiendo así a la red local de los atacantes externos.

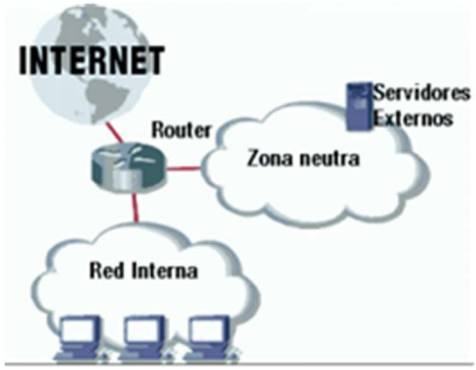


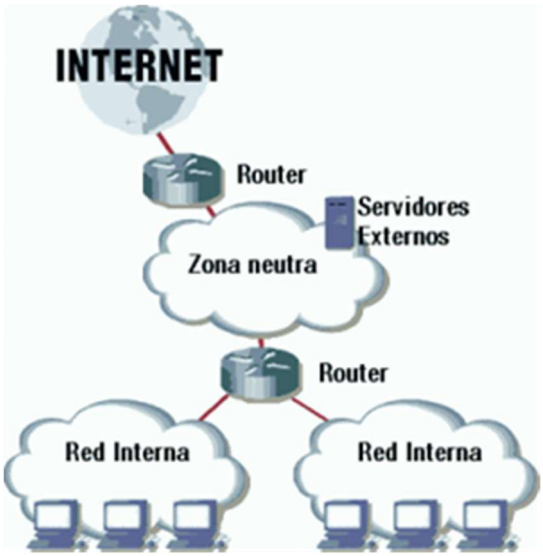
Al tener dos redes independientes se puede indicar a través de los routers el tráfico que se permite entre Internet y la zona neutra, o el tráfico entre la zona neutra y la red interna. Lo normal es que el router exterior esté configurado para permitir el acceso desde Internet a los servidores de la zona neutra, especificando los puertos utilizados, mientras que el router interior permite únicamente el tráfico saliente de la red interna al exterior. De esta forma si se produce un fallo de seguridad y se accede a los servidores de la zona neutra, el atacante nunca podrá tener acceso a la red interna de la empresa.

A partir del esquema de red con una red interna y una zona neutra puedes realizar las modificaciones que estimes oportunas para adaptarlo a tus necesidades. A continuación, a modo de ejemplo, se muestran algunas de las configuraciones más utilizadas:

2.3. Esquema de red con una zona neutra y una red interna utilizando un único router.

Aunque lo recomendable es utilizar dos routers para separar las redes también puede crear el esquema de red con un único router. En este caso el router tiene tres interfaces de red que le permiten crear la red interna, la zona neutra y conectarse a Internet. Aunque este esquema no es tan fiable como el anterior resulta más aconsejable que el modelo básico que no tiene ninguna zona neutra.



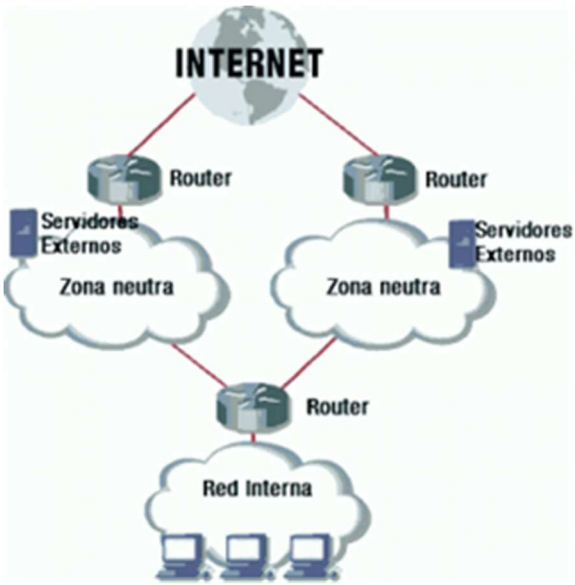


2.4. Esquema de red con una zona neutra y varias redes internas.

En los esquemas de red anteriores se ha creado una única red interna y por lo tanto todos los equipos y servidores internos están en la misma red dificultando así su seguridad. En el caso de que se tengan equipos con diferentes tipos de seguridad o servidores internos, resulta aconsejable crear varias redes internas para mejorar así la seguridad de la red. En la siguiente figura puede ver un esquema de red que tiene dos redes internas.

2.5. Esquema de red con varias zonas neutras.

En el caso de que la empresa necesite dar servicios bien diferenciados al exterior puede optar por tener dos zonas neutras, o incluso dos salidas diferentes a Internet. Por ejemplo, en el esquema de red de la figura tiene dos zonas neutras y dos salidas a Internet. En este caso una de las zonas neutras se puede utilizar para ubicar los servidores públicos (por ejemplo, un servidor web o ftp) y la otra zona neutra se puede utilizar para que los clientes se conecten por VPN a la red interna de la empresa. De esta forma, los clientes en la VPN estarán en una zona neutra que se encuentra aislada de la red de servidores públicos y la red interna.



2.6. Redes inalámbricas.

Las redes de área local inalámbricas (WLAN, Wireless Local Area Networks) permiten que varios dispositivos puedan transmitir información entre ellos a través de ondas de radio sin

necesidad de cables. Las ventajas saltan a la vista. La principal es la libertad que proporcionan a los usuarios de red, que pueden llevar su ordenador (especialmente si es portátil) a cualquier sitio sin perder la conexión a Internet.

El acceso sin necesidad de cables es la razón por la que son tan populares las redes inalámbricas, y es a la vez el problema más grande de este tipo de redes en cuanto a la seguridad se refiere. Cualquier equipo que se encuentre cerca del punto de acceso podrá tener acceso a la red inalámbrica.

Para poder considerar una red inalámbrica como segura debería cumplir los siguientes requisitos:

Aislar la red inalámbrica de la red interna de la empresa creando una zona neutra.

Al utilizar una zona neutra es posible limitar el acceso desde la red inalámbrica a los servicios y/o equipos que estime oportunos. Por ejemplo, una opción muy útil es permitir el acceso de la red inalámbrica únicamente a Internet o algún determinado servicio de la red interna.

- Las ondas de radio deben confinarse tanto como sea posible.
- Los datos deben viajar cifrados para impedir que sean capturados por otro equipo. Como ya has estudiado en la unidad anterior, para que los datos vayan cifrados existen dos protocolos de encriptación:
  - **WEP (Wired Equivalent Privacy)**. WEP fue el primer protocolo de encriptación introducido en el primer estándar 802.11 en el año 1999. Está basado en algoritmo RC4 con una clave secreta de 40 ó 104 bits, combinado con un vector de inicialización (IV:initialization vector) de 24 bits.
  - **WPA (WiFi Protected Access)**. Es un estándar creado para corregir los fallos de seguridad del protocolo WEP. Fue diseñado para utilizar un servidor de autentificación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK: Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.

Debe existir algún mecanismo de autentificación en doble vía que permita al cliente conectarse realmente a su punto de acceso, y que permita verificar que al punto de acceso sólo se conectan los clientes legítimos. Para permitir la autentificación de los clientes es posible utilizar un servidor de autentificación Radius.

Filtrado de dirección MAC. Un mecanismo adicional de seguridad es permitir el acceso a la red inalámbrica únicamente a unos determinados equipos. Para indicar los equipos que pueden acceder a la red inalámbrica se utiliza la dirección física (MAC) del adaptador de red.

3. Configuración de routers.

Como hemos visto anteriormente, un router es un dispositivo de interconexión que permite regular el tráfico que pasa entre varias redes. Un router es muy útil a la hora de defendernos de posibles intrusiones o ataques externos. Pero como desventaja es que un router no se configura por sí sólo. Mientras que un router bien configurado puede ser muy útil, un router mal configurado no nos proporciona ningún tipo de protección o, simplemente, no llega a comunicar dos redes.

3.1. Tablas de enrutado y filtrado.

Para configurar un router debemos crear lo que se denomina “tabla de enrutado” o "directivas de firewall". En ella se guardan las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino. Existen dos tipos de encaminamiento: **encaminamiento clásico y encaminamiento regulado.**

Con el **encaminamiento clásico**, las reglas utilizadas para encaminar los paquetes se basan, exclusivamente, en la dirección destino que aparece en la cabecera del paquete. Así se distinguen las siguientes reglas:

- Permitir un equipo de nuestra red.
- Permitir cualquier equipo de nuestra red.
- Permitir un equipo de otra red.
- Permitir cualquier equipo de otra red.
- La última regla (por defecto) se aplica en el caso de que no se cumpla ninguna de las anteriores y se suele utilizar para poder enviar los mensajes a la puerta de enlace de la red.

Sin embargo, en la actualidad, con la explosión del uso de Internet y la llegada del concepto de calidad de servicio (QoS) y la seguridad, los routers utilizan el llamado **encaminamiento regulado,** con el que, a la hora de escribir la tabla de enrutado, se pueden utilizar los siguientes elementos:

- **Interfaz**: interfaz de red por donde se recibe la información.
- **Origen** / **Destino:** origen y destino del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP, pero algunos routers permiten utilizar como dirección origen y destino usuarios o grupos de usuarios.
- **Protocolo:** permitir o denegar el acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto para que un cliente (que inicia la conexión) pueda conectarse. Por ejemplo un servidor web trabaja en el puerto 80, un servidor de FTP en el puerto 21, etcétera.
- **Seguimiento:** indica si el router debe de realizar un seguimiento de los lugares por los que pasa un mensaje.
- **Tiempo:** espacio temporal en el que es válida la regla.
- **Autentificación de usuarios:** indica si el usuario debe de estar autentificado para utilizar la regla.
- **Acción:** especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:
  - **Aceptar:** dejar pasar la información.
  - **Denegar:** no deja pasar la información.
  - **Reenviar:** envía el paquete a una determinada dirección IP.

Ejemplo de reglas de iptables

```
[root@redhatserver root]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.0/24          anywhere            tcp dpt:http
ACCEPT     udp  --  10.0.0.0/24          anywhere            udp dpt:domain
ACCEPT     all  --  anywhere             anywhere            state ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
[root@redhatserver root]#
```

3.2. Elementos de configuración de un router.

Existen diferentes tipos de routers por lo que en un principio podemos caer en la tentación de pensar que el proceso de configuración para cada router es totalmente diferente a los demás. Pero entre los router más utilizados, ya sean hardware o software, tenemos:

- FireWall 1 de CheckPoint.
- Private Internet Exchange (PIX) de Cisco System.
- IOS Firewall Feature Set de Cisco System.
- Firewall del núcleo de Linux, Iptables.
- Enterprise Firewall de Symantec.
- Internet Security and Acelerador (ISA Server) de Microsoft.

Si se comparan los elementos que utilizan los diferentes routers (ver tabla) puede ver cómo los más utilizados a la hora de realizar una tabla de enrutado son la **interfaz**, la **dirección origen** y **destino**, el **protocolo**, el **puerto** y la **acción** que debe realizar el router.

Comparativa sobre los elementos de las tablas de enrutado.							
Modelo	**Interfaz**	**Origen/destino**	**Protocolo**	**Seguimiento**	**Tiempo**	**Autentificación de usuarios**	**Acción**
FireWall 1	√	√**	√	√	√		√
PIX	√	√	√*				√
IOS Firewall	√	√	√				√
Firewall Linux	√	√	√				√
Enterprise Firewall	√	√**	√		√	√	√
ISA Server	√	√**	√*		√	√	√

*Distingue entre puerto de origen y destino.
**Permiten especificar como origen o destino direcciones IPs o usuarios.

A la hora de indicar la **dirección de origen** o la **dirección de destino** es importante utilizar la máscara de red para indicar un mayor o menor número de ordenadores. Así por ejemplo, si en la dirección destino utiliza la dirección de clase B 142.165.2.0/16 se hace referencia a todas las direcciones IP del tipo 142.165.x.x. Si utiliza la dirección de clase C 192.165.2.0/24, hace referencia a las direcciones del tipo 192.165.2.x. Por lo tanto, si aumentamos la máscara de red, estamos disminuyendo el número de direcciones IP a las que se hace referencia y si disminuimos la máscara de red, entonces se hace referencia a un mayor número de direcciones IP. En la tabla siguiente, puedes ver algunas de las posibilidades más habituales.

Ejemplos de utilización de la máscara de red en la configuración de routers	
Ejemplo	**Comentario**
192.165.2.23/32	Representa a un único ordenador (por ejemplo, un servidor web)
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X

Durante el filtrado de paquetes se aplica la regla de “coincidencia total”. Todos los criterios de la regla tienen que coincidir con el paquete entrante; en caso contrario, no se aplica la regla. Esto no significa que se rechace el paquete o que se elimine, sino que la regla no entra en vigor. Normalmente, las reglas se aplican en orden secuencial, de arriba hacia abajo. Aunque hay varias estrategias para implementar filtros de paquetes, las dos que se describen a continuación son las más utilizadas por los especialistas de seguridad:

- **Construir reglas desde la más específica a la más general.** Esto se hace así para que una regla general no "omita" a otra más específica, pero conflictiva, que entra dentro del ámbito de la regla general.
- **Las reglas deberían ordenarse de tal forma que las que más se utilizan estén en la parte superior de la lista.** Esto se hace por cuestiones de rendimiento. Normalmente un router detiene el procesamiento de una lista cuando encuentra una coincidencia total.

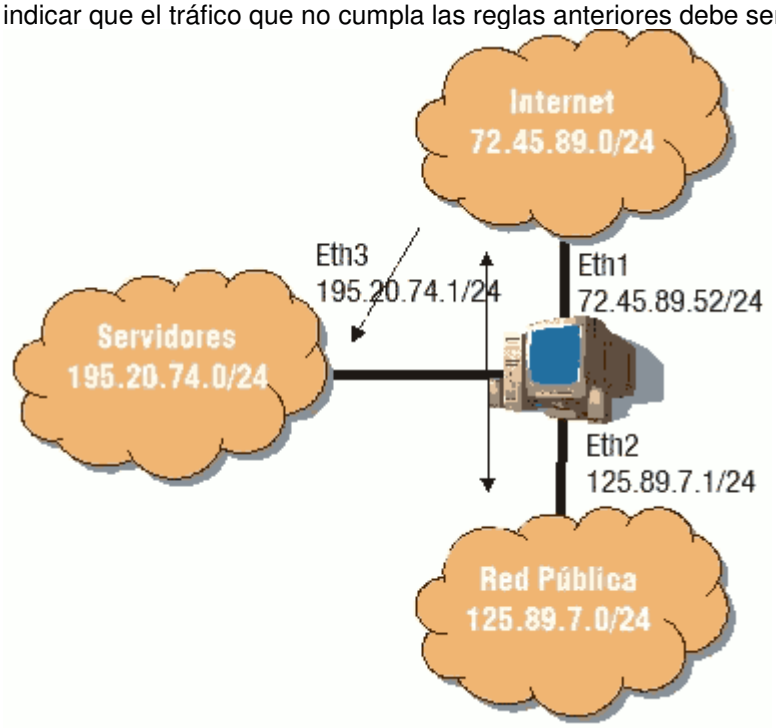
3.3. Ejemplo de creación de una tabla de enrutado.

La figura muestra un router conectado a tres redes diferentes. Debemos crear el conjunto de reglas para permitir que: la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

La tabla de enrutado representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes. Las notas acerca de la implementación se incluyen siguiendo la descripción de cada línea del conjunto de reglas.

Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.



Ejemplo de red

Tabla de enrutamiento					
Reglas	**Interfaz**	**Origen**	**Destino**	**Puerto**	**Acción**
1	Eth1	72.45.89.0/24	195.20.74.5/32	80	Aceptar
2	Eth1	72.45.89.0/24	195.20.74.7/32	25, 110	Aceptar
3	Eth1	72.45.89.0/24	195.20.74.0/24	-	Denegar
4	Eth1	72.45.89.0/24	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	72.45.89.0/24	-	Aceptar
6	-	0.0.0.0/0	0.0.0.0/0	-	Denegar

Regla 1. Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 195.20.74.5 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.

Regla 2. Esta regla permite el acceso entrante a los puertos 25 y 110, que normalmente se utiliza para correo electrónico (el puerto 25 es el servidor smtp o correo saliente y el puerto 110 es el servidor pop3 o correo entrante). El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, como no se puede predecir quién va a tener acceso al servidor de correo no se restringen las direcciones IP de origen.

Regla 3. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a ningún servidor.

Reglas 4 y 5. La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.

Regla 6. Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.

4. Servicios de red.

Aunque los servicios más conocidos en Internet son el servidor Web y el de correo electrónico, también existen otros servicios necesarios y menos conocidos que permiten crear la infraestructura de una red. Estos servicios son los siguientes:

- Encaminamiento. Permite a un servidor actuar como router para permitir la comunicación entre dos o más redes.
- Servidor DHCP. Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando un portátil se conecta a una red obtiene su configuración IP a través de un servidor DHCP.
- Servidor DNS. Permite mantener una equivalencia entre un nombre y su dirección IP. Por ejemplo, el nombre www.adminso.es equivale a 150.214.150.30.

Además de los servicios ya comentados existen otros muchos servicios como, por ejemplo, compartir datos, acceso remoto a sistema, monitorización de equipos, etcétera. A continuación, se van a ver los servicios más utilizados.

Posteriormente, veremos los dominios de Internet y los servicios de Internet más importantes.

4.1. Servicio DHCP.

El mantenimiento y la configuración de la red de los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IPs, así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace…conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP; o se dispone de un sistema de asignación dinámica y flexible que permita reutilizar las direcciones

de tal forma que sólo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente que tenemos, algo inviable con el número de usuario conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

El servidor DHCP se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Para ello, necesita de un proceso (dhcpd) y un fichero de configuración (/etc/dhcpd.conf)

Los datos mínimos que un servidor de DHCP proporciona a un cliente son:

- Dirección IP.
- Máscara de red.
- Puerta de enlace o gateway.
- Dirección IP del servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- **Asignación dinámica.** Asigna direcciones IPs libres de un rango de direcciones establecido por el administrador en el fichero/etc/dhcpd.conf. Es el único método que permite la reutilización dinámica de las direcciones IP.
- **Reserva por dirección IP**. Si queremos que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración, para una determinada dirección MAC, se asignará una dirección IP. Este método es muy útil para aquellos dispositivos que no queramos que cambien de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP deberemos configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

4.2. Servicio DNS.

Los equipos informáticos se comunican entre sí mediante una dirección IP como 193.147.0.29. Sin embargo, nosotros preferimos utilizar nombres como www.mec.es porque son más fáciles de recordar y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.

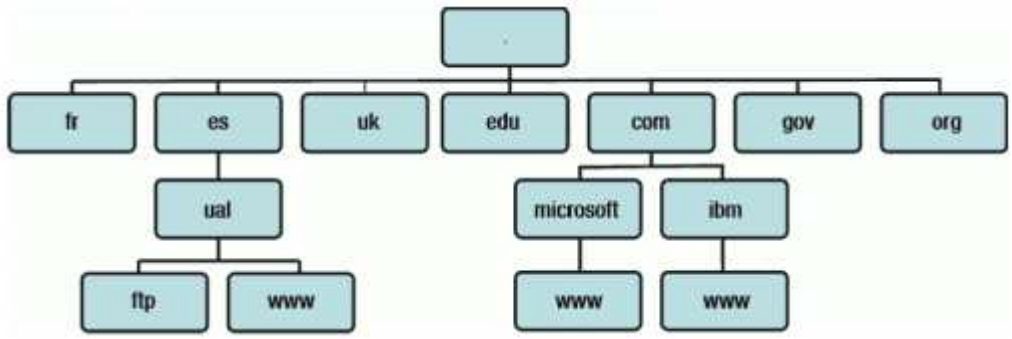
Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del fichero /etc/hosts (Linux) o \winnt\system32\driver\etc\hosts (Windows) en los que se guarda cada nombre junto a su respectiva dirección IP. Con todo, esta opción presenta varios problemas.

Por un lado, todos los equipos de la red están obligados a conocer cualquier cambio para actualizar sus ficheros apropiadamente. Es decir, ante, por ejemplo, la inserción de un nuevo elemento en la red, debe añadirse en los ficheros locales de cada equipo los datos referentes a su nombre y dirección IP. Este hecho indica la poca escalabilidad y manejabilidad de esta opción, sobre todo si hablamos de Internet o, sin llegar a este extremo, de cualquier red local que tenga, por ejemplo, más de veinte ordenadores. Además, el mantenimiento tan descentralizado y dependiente de ficheros locales conlleva un alto riesgo de falta de sincronización y descoordinación entre los equipos de la red y, por tanto, de la información que manejan.

Para paliar estos problemas se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se dispone de uno o más servidores encargados de resolver los nombres de los equipos pertenecientes a su ámbito, consiguiendo, por un lado, la centralización necesaria para la correcta sincronización de los equipos, un sistema jerárquico que permite una administración focalizada y, también, descentralizada y un mecanismo de resolución eficiente.

4.2.1. Espacio de nombres de dominio.

Al igual que los sistemas de fichero se organizan en árboles jerárquicos y el nombre absoluto de un fichero es el formado por los distintos directorios que recorremos hasta encontrar el fichero, separados por el carácter '/' (o '\' en sistemas Windows). El sistema de nombres de dominios también se estructura con un árbol jerárquico en el que las distintas ramas que encontramos reciben el nombre de dominio y el nombre completo de un equipo (el equivalente al nombre de un fichero) o FQDN (path absoluto) es el nombre resultante de recorrer todos los dominios por los que pasamos, desde las hojas hasta la raíz del árbol utilizando, en este caso, el carácter '.' (punto) como separador.



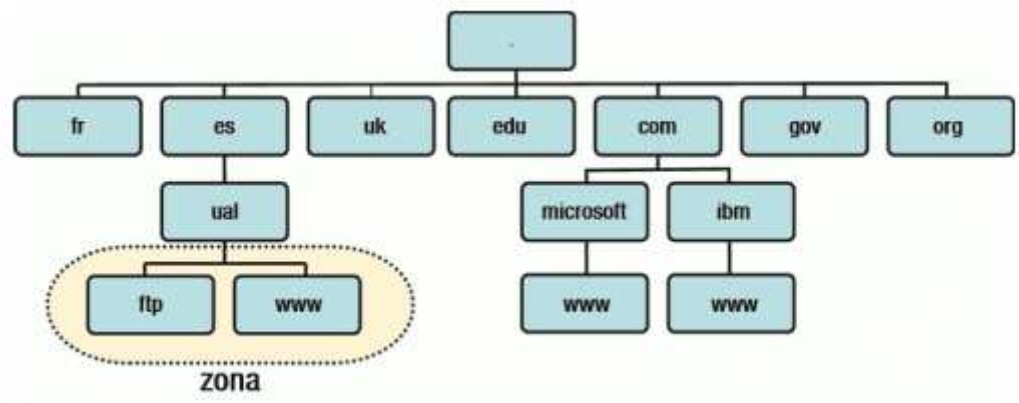
Ejemplo de jerarquía de los dominios en Internet

El sistema de nombres de Internet presenta, por tanto, una estructura jerárquica en árbol, en el que cada rama constituye lo que se denomina un dominio de Internet, y dependiendo de la profundidad del árbol, hablaremos de dominios de primer, segundo o tercer nivel –pudiendo existir más, aunque no es habitual-.

En el primer nivel del árbol encontramos que los nombres de los nodos ya están establecidos de antemano, existiendo dos tipos de divisiones: geográfica y organizativa. Con la primera se distingue una rama -dominio- por país: .es para España; **.uk** para Gran Bretaña; **.de** para Alemania, ... Con la segunda se establece una rama por tipo de organización: **.com** para empresas, independientemente del país en el que se encuentren; **.int** para organizaciones establecidas mediante tratados internacionales; **.org** para organizaciones no gubernamentales y, por último, **.edu**, **.gov** y **.mil** para organizaciones educativas, del gobierno y el ejército de EEUU. Posteriormente, se han introducido nuevos dominios de primer nivel como **.name** para nombres de personas; **.info** para proveedores de servicios de información; web para empresas relativas a servicios web; etcétera.

Cada rama del árbol jerárquico en el que se estructura el sistema de nombres de dominio, recibe el nombre de dominio y, para la resolución global de nombres no es determinante quién se encarga de mantener la información asociada a cada dominio. Con esta estructura, la asignación de nombres de una rama del árbol de primer nivel se delega en un responsable -la empresa pública REDES para España- el cual puede decidir, a su vez, delegar la autoridad de resolución de los nombres de las distintas ramas en las que se divide, en otras corporaciones.

Un servidor DNS puede encargarse de gestionar los datos de un dominio completo o parte de un dominio. El conjunto de datos que puede administrar un servidor de nombres recibe el nombre de zona. En la siguiente figura puede ver que el servidor DNS será el encargado de gestionar los datos del dominio **ual.es.**



Representación de una zona gestionada por un servidor

Por otra parte, con la importancia que ha adquirido la resolución de nombres -nadie usa ya las direcciones IP, sino los nombres asociados- una característica crucial es la máxima disponibilidad del servicio. Para ello, una buena solución es que existan varios servidores independientes capaces de realizar el mismo servicio de tal forma que la autoridad de resolución de zona siga recayendo en un servidor, aunque éste puede permitir que otros puedan responder a requerimientos de los clientes. Los servidores que tienen asignada la autoridad de resolución de nombres y que gestionan la base de datos de la zona, reciben el nombre de servidores primarios. Los servidores que pueden resolver requerimientos para una zona, pero que la fuente de información la obtienen de otro servidor, reciben el nombre de servidores secundarios.

Para que no existan problemas de sincronización entre servidores, los secundarios deben conseguir sus datos del servidor primario mediante el proceso llamado “transferencia de zona” que no es más que el traspaso de todas los pares dirección IP-nombre simbólico que gestiona el servidor. Cada vez que se modifique un dato del servidor primario debe transmitirse a todos los secundarios que estén declarados para el correcto funcionamiento del sistema.

De esta forma, no sólo se consigue aumentar la disponibilidad del servicio, sino hacerlo más eficiente ya que la carga de trabajo puede repartirse entre distintos servidores. Si el objetivo es exclusivamente éste, existe otro tipo de servidores llamados caché cuya finalidad es la de responder a peticiones de resolución, consultando, previamente, las peticiones almacenadas en memoria y, si no se corresponde con ninguna de ellas, iniciar el proceso de resolución de nombres recursivo visto anteriormente. Los servidores caché sólo son útiles si el número de usuarios es suficientemente elevado para sacar provecho de la caché de direcciones.

4.2.2.Registrar un dominio.

Cualquier persona física con residencia en España, así como empresas constituidas según la legislación española, puede solicitar el registro de dominios a través de la página nic.es o bien, por medio de los agentes registradores acreditados. Los nombres de dominio se deben, según la reglamentación española, corresponder con:

- Nombre (o abreviatura) de una empresa que la identifique de forma inequívoca.
- Nombres comerciales o de marcas.
- Nombre de personas tal y como aparecen en su DNI, con un máximo de 60 caracteres.
- Nombres de profesiones y el apellido o nombre del profesional que se dedica a dicha labor o del nombre del establecimiento.
- Denominaciones de origen, en cuyo caso debe solicitarlo el órgano regulador de dicha denominación.

Una vez registrado el dominio podremos acceder a una web que nos permitirá gestionar los distintos registros del dominio.

4.2.3. Tipos de registro.

Tal y como hemos visto anteriormente, un servidor de nombres es el encargado de gestionar un dominio o parte de un dominio. El conjunto de datos que administra el servidor recibe el nombre de zona. Por ejemplo, el servidor de nombres del Ministerio de Educación es el encargado de gestionar la zona **mec.es**.

Para administrar una zona existe un servidor DNS primario y normalmente, además del servidor primario se dispone de uno o más servidores secundarios que únicamente realizan una copia de la zona.

La comunicación entre los servidores DNS se realizan mediante lo que se llama una transferencia de zona. Una zona (por ejemplo, **mec.es**) tiene registros DNS (por ejemplo, www.mec.es) que son los encargados de asociar un nombre a una dirección IP. En la tabla se muestran los diferentes tipos de registros DNS de un servidor de nombres entre los que se destacan:

- Registro tipo A. Es el más utilizado y permite asociar un nombre (por ejemplo, www.mec.es) con una dirección IP (por ejemplo: 193.147.0.29).
- Registro tipo CNAME. Permite establecer un alias entre dos registros. Por ejemplo, www.mec.es es igual que ftp.mec.es.
- Registro MX. Este registro es muy importante ya que permite indicar dónde se encuentra el servidor de correo electrónico (Mail eXchanger). Este tipo de registro se asocia siempre a otro nombre y permite asignar prioridades en los servidores. Así la entrada MX10 indica el primer servidor de nombres, MX20 el segundo, etcétera.

Tipos de registro	
Registro	**Función**
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.
HINFO	Descripción de la computadora. CPU y S.O.
WKS	Servicios públicos disponibles en la computadora.

4.3. Servicio FTP.

FTP es el protocolo más antiguo de la capa de aplicación TCP/IP que permite la transferencia de ficheros. FTP define un protocolo cliente/servidor que describe la manera en que se establece la comunicación entre los servidores y clientes FTP. Concretamente, permite el envío y la recepción de archivos del servidor.

Aunque pueden contemplarse otras posibilidades, hay dos tipos fundamentales de acceso a través de FTP:

- **Anónimo**. La comunicación se realiza sin ningún tipo de identificación y, por lo tanto, el usuario tendrá muy pocos privilegios en el servidor. En este caso, el usuario estará confinado en un directorio público donde puede descargar los archivos allí ubicados, pero sin posibilidad de escribir o modificar ningún fichero.
- **Acceso autorizado**. El usuario establece la comunicación con una cuenta de usuario. Tras identificarse, se confina al usuario a su directorio predeterminado desde donde puede descargar ficheros y, si la política del sistema lo permite, también escribir. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.

Existen programas que permiten conectarse cómodamente a un servidor FTP (por ejemplo: filezilla, cuteftp, vsftp, Internet Explorer). Sin embargo, la forma más simple de utilizar un servidor FTP es estableciendo una conexión por línea de comandos. Para poder conectarte a un servidor puedes ejecutar ftp servidor en el intérprete de comandos de tu sistema, y utilizado los comandos

FTP que aparecen en la tabla de comandos de FTP, sin importar el sistema operativo que utilices, puedes trabajar en el servidor FTP.

4.4. Servicio Web.

Conocido con el nombre de World Wide Web, o más concretamente, por sus siglas WWW que, además, aparecen en el nombre de prácticamente todos los servidores web, el servicio web es, posiblemente, el servicio más extendido y utilizado de los que se ofrecen en Internet, con el permiso del sistema de correo electrónico.

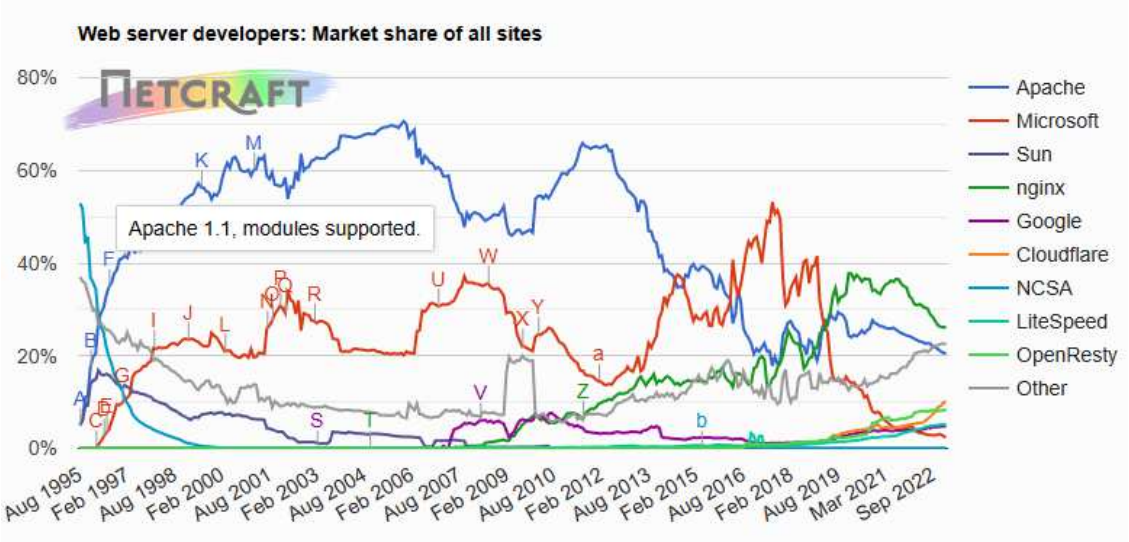
El servidor web se encarga del almacenaje y la difusión de información mediante la distribución de páginas HTML. Su arquitectura se basa en la archiconocida cliente-servidor, típica de los servicios basados en TCP/IP, en la que se distinguen: el proceso servidor, como, por ejemplo, Apache, Internet Information Server e Iplanet y el proceso cliente (también llamado navegador), como Mozilla Firefox, Google Chrome, Internet Explorer, etcétera.

El servidor es el que almacena y sirve las páginas HTML. Los navegadores se encargan, además de realizar la petición de la página deseada, de interpretarla y mostrar el resultado al usuario. Para que el cliente y el servicio se entiendan, se comunican mediante el protocolo HTTP. Este es un protocolo orientado a conexión y del tipo de solicitud-respuesta, es decir, no se guarda información de estado, sino que toda interacción entre el cliente y el servidor se fundamenta en pedir y servir.

Para identificar qué página desea un cliente, éste realiza una petición con la que especifica toda la información necesaria para que tanto el navegador como el servidor web interpreten correctamente qué recurso desea el cliente y dónde se encuentra. La petición se realiza mediante el llamado localizador universal de recursos (URL).

Para solicitar páginas y visualizarlas, los clientes web (navegadores) presentan un entorno gráfico y amigable que facilita la navegación por la WWW. Existen multitud de navegadores con la misma funcionalidad y, prácticamente, con las mismas características. Las principales diferencias entre los clientes web residen en el número e importancia de vulnerabilidades que presentan, así como en diferentes matizaciones que existen en cuanto a la interpretación del código HTML y que puede impedir la correcta visualización de algunas páginas en determinados clientes. Ejemplos de clientes Google Chrome, Internet Explorer, Firefox u Opera.

En la actualidad existen varios servidores Web tanto para sistemas GNU/Linux como para sistemas Windows. Como se observa en la siguiente gráfica, Apache es el servidor Web más utilizado en Internet muy por encima del resto de competidores.



https://news.netcraft.com/

4.5. Servicio de correo electrónico.

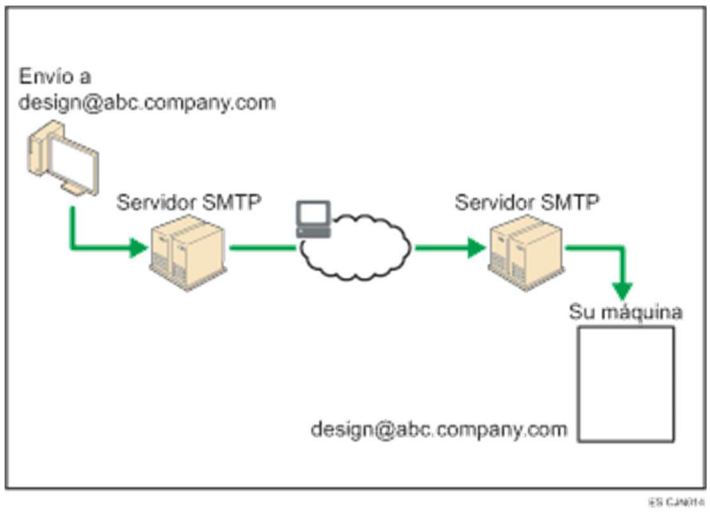
El sistema de correo electrónico es, junto al WWW, el servicio proporcionado en Internet que más importancia y auge ha presentado, al menos en cuanto al número de usuarios se refiere. De hecho, se considera como uno de los principales factores que ha popularizado el uso de Internet.

Este servicio es un sistema para la transferencia de mensajes, rápido y eficiente, ideado bajo la arquitectura cliente-servidor típica de Internet. No es simplemente un programa cliente que se comunica con un servidor mediante un protocolo de aplicación, sino que está compuesto por varios subsistemas, cada uno con una funcionalidad determinada que interaccionan entre sí mediante distintos protocolos de aplicación. La funcionalidad que todo usuario espera de este sistema es:

- Composición del mensaje.
- Transferencia desde el origen al destino sin intervención del usuario.
- Generación de un informe de la transmisión del mensaje.
- Visualización de los correos recibidos.
- Gestión de los correos: lectura, borrado, almacenaje...

Otras características que puede aportar un sistema de correo electrónico a un usuario son, por ejemplo, la redirección de correos de unas cuentas a otras, listas de correo, correo de alta prioridad o cifrado... El sistema de correo electrónico lo constituyen cuatro componentes:

- Cliente de correo electrónico (MUA). Ofrece los mecanismos necesarios para la lectura y composición de los mensajes de correo. Este componente esta replicado, en el emisor y en el receptor.
- Servidor de correo saliente (MTA). Recibe el correo electrónico y lo envía al servidor de entrada del dominio del receptor. Normalmente utiliza los protocolos SMTP o IMAP.
- Servidor de correo entrante (MDA). Almacena los correos electrónicos enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido. Normalmente utiliza los protocolos POP o IMAP.



Arquitectura del sistema de correo electrónico

Para comunicar los distintos subsistemas que componen la arquitectura del servicio de correo, se dispone de los protocolos:

- Simple Mail Transport Protocol (SMTP) encargado del transporte de los mensajes de correo.

- Postal Office Protocol (POP) e Internet Message Access Protocol (IMAP) encargados, ambos, de comunicar a los agentes de usuario (MUA) con los agentes de entrega de correo (MDA). Además, permiten la gestión, por parte de los usuarios, de sus buzones de correo.

El cliente de correo electrónico es una aplicación que proporciona al usuario una interfaz -más o menos amigable- con los mecanismos necesarios para escribir, recibir y contestar a mensajes.

Cuando el MUA es un programa instalado en el sistema del usuario, se llama cliente de correo electrónico (tales como Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail o Lotus Notes).

Cuando se usa una interfaz de web para interactuar con el servidor de correo entrante, se llama correo electrónico.

Existen clientes de correo electrónico basados en diferentes interfaces, de texto o gráfica, que introducen más o menos familiaridad y coste de aprendizaje para el usuario, pero todos presentan las mismas funciones: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.

4.6. Servicio de acceso remoto.

Los servicios que permiten acceder de forma remota a un equipo a través de la red. Los servicios de acceso remoto se clasifican en dos categorías:

- **Acceso remoto en modo terminal.** Para acceder a un servidor GNU/Linux en modo terminal es posible utilizar los servicios Telnet (Telecommunication NETwork) y SSH (Secure SHell). Actualmente el servicio SSH es el más utilizado ya que garantiza la seguridad de las comunicaciones mientras que el servicio Telnet no se utiliza por ser inseguro.

- **Acceso remoto en modo gráfico.** Para acceder en modo gráfico a un servidor puede utilizar el servicio VNC (Windows y GNU/Linux) o el servicio de Escritorio remoto (o Terminal Server) en sistemas Windows.